SPECTRUM®

Portable Management Application for the 7C03, 7C04, and 7C04-R SmartSwitch Hubs

User's Guide

CABLETRON SYSTEMS Inc.

The Complete Networking Solution

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Virus Disclaimer

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © 1996 by Cabletron Systems, Inc. All rights reserved.

Printed in the United States of America.

Order Number: 9031977-E1 October 1996

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

SPECTRUM, **MiniMMAC**, **FNB**, **Multi Media Access Center**, and **DNI** are registered trademarks, and **Portable Management Application**, **IRM**, **IRM2**, **IRM3**, **IRBM**, **ESXMIM**, **ETSMIM**, **EMME**, **EMM-E6**, **ETWMIM**, **FDMMIM**, **FDCMIM**, **MicroMMAC**, **MRXI**, **MRXI-24**, **NB20E**, **NB25E**, **NB30**, **NB35E**, **NBR**, **SEHI**, **STHI**, **TRBMIM**, **TRMM**, **TRMM-2**, **TRMM-4**, **TRMMIM**, **TRXI**, **Media Interface Module**, **MIM**, and **Flexible Network Bus** are trademarks of Cabletron Systems, Inc.

UNIX and **OPENLOOK** are trademarks of Unix System Laboratories, Inc. **OSF/Motif** and **Motif** are trademarks of the Open Software Foundation, Inc. **X Window System** is a trademark of X Consortium, Inc. **Ethernet** and **XNS** are trademarks of Xerox Corporation. **Apple** and **AppleTalk** are registered trademarks of Apple Computer, Inc. **Banyan** is a registered trademark of Banyan Systems, Inc. **DECnet** is a registered trademark of Digital Equipment Corporation. **Novell** is a registered trademark of Novell, Inc. **CompuServe** is a registered trademark of CompuServe. **Sun Microsystems** is a registered trademark, and **Sun**, **SunNet**, and **OpenWindows** are trademarks of Sun Microsystems, Inc.

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

   Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.

   (b) This computer software may be:

      (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;

      (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;

      (3) Reproduced for safekeeping (archives) or backup purposes;

      (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;

      (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and

      (6) Used or copied for use in or transferred to a replacement computer.

   (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

   (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.

   (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

Contents

Chapter 1 Introduction to SPMA for the 7C0x SmartSwitch

Using the 7C0x SmartSwitch User's Guide 1-2
What's NOT in the 7C0x SmartSwitch User's Guide 1-4
Conventions 1-5
Screen Displays 1-5
Using the Mouse 1-7
Getting Help 1-8
7C0x SmartSwitch Firmware 1-8

Chapter 2 Using the 7C0x SmartSwitch Hub View

Using the Hub View 2-1
Navigating Through the Hub View 2-2
Hub View Front Panel 2-3
Using the Mouse in a Hub View Module 2-4
Monitoring Hub Performance 2-5
Selecting the Application Display Mode 2-6
COM Port and FDDI Front Panel Displays 2-8
FDDI Port Display Forms 2-8
FDDI Color Codes 2-10
The Switch Application Display 2-10
Switch Port Display Forms 2-11
Switch Port Color Codes 2-12
The Bridge Application Display 2-13
Bridge Port Display Forms 2-13
Bridge Port Color Codes 2-15
The Interface Application Display 2-15
Interface Port Display Forms 2-16
Interface Port Color Codes 2-20
Viewing Device Configuration 2-20
Viewing the Interface List 2-22
Viewing Switch Status 2-23
Viewing the Source Address List 2-24
Managing the Hub 2-25
Launching SPMA Tools from the Hub View 2-25
Module Utilities 2-26
MIB I, II 2-26

Find MAC Address 2-26
UPS 2-27
Accessing FDDI Management 2-27
Accessing ATM Management 2-28
Accessing Bridge Management 2-28
Setting the Polling Intervals 2-28
Port Configuration 2-30
Configuring Ethernet and FDDI Ports 2-30
Configuring Fast Ethernet Ports 2-32
Setting the Desired Operational Mode 2-35
Configuring COM Ports 2-36
Enabling and Disabling Bridge Ports 2-38

Chapter 3 Basic Alarm Configuration

About Basic Alarms 3-1
Launching the Basic Alarm Application 3-2
Viewing Alarm Status 3-3
How Rising and Falling Thresholds Work 3-6
Configuring an Alarm 3-7
Disabling an Alarm 3-9
Viewing an Alarm Log 3-10

Chapter 4 FDDI Management

Port Configuration 4-2
Enabling or Disabling FDDI Ports 4-5
Charts, Graphs, and Meters 4-5
Viewing the FDDI Port Chart 4-6
Changing the Measurement of Data 4-7
Viewing FDDI Port Meters 4-7
Viewing FDDI Port Graphs 4-8
Alarm Configuration 4-9
SMT/MAC Configuration 4-13
Charts, Graphs, and Meters 4-17
Viewing the FDDI MAC Chart 4-18
Changing the Measurement of Data 4-19
Viewing FDDI MAC Meters 4-19
Viewing FDDI MAC Graphs 4-20
Configuring the SMT Connection Policy 4-21
FDDI Connection Rules 4-22
Special Ring Configurations 4-23
Defining Your Connection Policy 4-23
Viewing the Station List 4-24

Chapter 5 ATM Configuration

Accessing the AToM MIB Window 5-1
Configuring Connections 5-4

Chapter 6 Using the 7C0x SmartSwitch Bridge View

Bridging Basics 6-1
Transparent Bridging 6-2
Accessing the Bridge Traffic View Window 6-2
Navigating Through the Bridge Traffic View 6-3
Bridge Traffic View Front Panel 6-4
The Bridge Port Display 6-6
Choosing Bridge Traffic Information: Bridge Traffic View Buttons 6-6
Using the Detail View Window 6-8
Changing Ports in the Detail View 6-10
The Bridge Status Window 6-11
The Bridge Statistics Window 6-11
The Filtering Database Window 6-13
Viewing the Filtering Database 6-14
Changing the Filtering Database Dynamic Ageing Time 6-17
Changing Forwarding and Static Database Entries 6-18
Deleting a Static Table Entry 6-19
Finding a Filtering Database MAC Address 6-20
The Spanning Tree Protocol Window 6-20
Changing Spanning Tree Parameters 6-24
The Spanning Tree Port Parameters Window 6-25
Changing a Port's STA Parameters 6-27
Creating Bridge Traffic Charts, Graphs, and Meters 6-27
The Bridge Port Forwarding Statistics Window 6-28
Port Forwarding Statistics Window Fields 6-29
Configuring Forwarding Thresholds 6-30
Viewing the Forwarding Log 6-33
Changing Polling Intervals 6-35
Enabling and Disabling Ports 6-36
Enabling and Disabling a Transparent Bridge Port 6-36

Appendix A 7C0x SmartSwitch MIB Structure

IETF MIB Support A-1
7C0x SmartSwitch MIB Structure A-1
A Brief Word About MIB Components and Community Names A-3

Index

Chapter 1

Introduction to SPMA for the 7C0x SmartSwitch

How to use the 7C0x SmartSwitch User's Guide; manual conventions; contacting Cabletron Technical Support; 7C0x SmartSwitch firmware versions supported by SPMA

Your SPMA for the 7C0x SmartSwitch management module provides management support for all three models in the 7C0x SmartSwitch family. The **7C03 MMAC SmartSwitch** functions as a chassis within a chassis; residing in an MMAC-series hub, it occupies two module slots and provides three slots of its own — one for the 7X00 SmartSwitch Control Module, and two for its own family of Network Interface Modules, or NIMs. The **7C04 Workgroup SmartSwitch** is a stand-alone chassis that offers four slots: one for the controller, and three for NIMs. The **7C04-R Workgroup SmartSwitch** supplies all the features of the 7C04 along with the additional fault tolerance provided by a pair of redundant load-sharing power supplies and a removable fan tray. The 7C04-R can also accept the new double-wide NIM modules (in slots 3 and 4) for additional front panel connectivity.

TIP

The 7C03 MMAC SmartSwitch chassis provides no network connection to the MMAC backplane (from which it draws only power). If you wish to connect one or more networks from the MMAC chassis to the SmartSwitch chassis, you must do so via the front panel ports available on both the MMAC MIMs and the SmartSwitch NIMs.

At the heart of each 7C0x SmartSwitch hub is its 7X00 SmartSwitch Control Module, which supervises access to the switching backplane and performs all forwarding, filtering, and connection management functions; a variety of NIM modules provide connectivity for FDDI, Ethernet, Fast Ethernet, and ATM networks. NIM modules currently available include:

- The **7E03-24**, a single-slot Ethernet module that provides 24 ports via two RJ71 connectors.
- The **7E02-24**, a double-wide Ethernet module for the 7C04-R which provides 24 ports via RJ45 connectors.
- The **7F06-02**, which provides connectivity for two FDDI ring networks via its two front-panel FPIM slots; FPIM modules that support both multi-mode fiber and single-mode fiber (both with MIC connectors) and both shielded and unshielded twisted pair (with RJ45 connectors) are available.
- The **7H02-06**, which provides six Fast Ethernet connections — the first via a Fast Ethernet Port Interface Module slot, and an additional five via built-in Category 5 UTP RJ45 connectors. Two Fast Ethernet port modules are available: the FE-100FX, which provides a single multi-mode fiber port with an SC connector; and the FE-100TX, with a single Category 5 UTP RJ45 connector.
- The **7H02-12**, a double-wide module which provides 12 Fast Ethernet connections — the first via a Fast Ethernet Port Interface Module slot, and another 11 via built-in UTP RJ45s.
- The **7H06-02** Fast Ethernet uplink module, which provides two Fast Ethernet connections via Fast Ethernet Port Interface Module slots.
- The **7A06-01**, which provides a redundant ATM uplink connection via two front panel ATM Port Interface Module slots. Available APIMs provide connectivity for all standard ATM speeds and media types.

The available modules provide your SmartSwitch hub with key mission-critical features such as redundant links, alarm thresholding, and full error breakdown; Ethernet modules also provide per-port RMON support. By default, the 7X00 performs traditional switching (or bridging); depending on the version of firmware you have installed, the 7X00 module can also be configured to perform Cabletron's SecureFast switching.

NOTE

Not all released firmware versions support the ability to select SecureFast switching; check your hardware manuals to see if your version of firmware supports this feature. Currently, the toggle from traditional bridging to SecureFast switching is performed via Local Management; see your Local Management documentation for details.

Note that because the 7C03, 7C04, and 7C04-R provide the same functionality and support the same family of NIM modules (with the exception of the double-wide modules, which can be installed only in a 7C04-R), they will be referred to collectively throughout this manual as the 7C0x SmartSwitch. Where significant differences exist, they will be noted.

Using the 7C0x SmartSwitch User's Guide

Your SPECTRUM Portable Management Application (SPMA) for the 7C0x SmartSwitch consists of a number of different applications, each of which provides a portion of the overall management functionality. Each of these applications can be accessed from the icon menu (if you are using a management platform) and from the Stand-alone Launcher or the command line (if you are running in stand-alone mode); in addition, several applications can also be accessed from within the Hub View, a graphical display of the 7C0x SmartSwitch hub and its installed modules.

The 7C0x SmartSwitch ***User's Guide*** describes how to use many of the applications included with the module; note that the instructions provided in this guide apply to the 7C0x SmartSwitch module regardless of the operating system or management platform you are using. Instructions for launching each individual function from the command line (stand-alone mode) are also included in each chapter.

Following is a description of the applications covered in this guide; while we provide as much background information as we can, we do assume that you're familiar with Ethernet, Fast Ethernet, FDDI, and ATM networks, traditional bridging and switching, and with general network management concepts:

- Chapter 1, **Introduction to SPMA for the 7C0x SmartSwitch**, describes the 7C0x SmartSwitch ***User's Guide*** and the conventions used in this and other SPMA manuals, explains where to find information about the 7C0x SmartSwitch, and tells you how to contact Cabletron Systems Technical Support.
- Chapter 2, **Using the 7C0x SmartSwitch Hub View**, describes the visual display of the Hub and explains how to use the mouse within the Hub View; some basic functions (changing the Hub View display, opening menus and windows, enabling and disabling bridge ports, and so on) available only from within the Hub View are also described. You can access the Hub View application from the icon menu or the command line.
- Chapter 3, **Alarm Configuration**, describes how the 7C0x's RMON functionality allows you to set thresholds and enable or disable alarms for any installed bridging interface based on selected MIB II statistics; this chapter also describes how to specify a response to an alarm condition. You can access the Alarm Configuration application from the icon menu, the Hub View, or the command line.
- Chapter 4, **FDDI Management**, describes the five applications available for managing any installed FDDI interfaces. You can access the FDDI applications from the Hub View or the command line.
- Chapter 5, **ATM Configuration**, describes how to use the ATM configuration application to view and configure the Permanent Virtual Circuits supported by any installed 7A06-01 modules.

- Chapter 6, **Using the 7C0x SmartSwitch Bridge View**, provides detailed instructions for configuring and managing the 7C0x SmartSwitch's traditional bridging capabilities, including monitoring bridge operation, using the special and filtering data bases, and setting forwarding thresholds and notification options. You can access the Bridge View from the icon menu, the Hub View, or the command line.
- Appendix A, **7C0x SmartSwitch MIB Components**, lists the IETF MIBs supported by the 7C0x SmartSwitch, and describes their arrangement in a series of MIB components. A description of the objects controlled by each component is also included.

What's NOT in the 7C0x SmartSwitch User's Guide . . .

The following standard SPMA tools are available through the 7C0x SmartSwitch module and are explained in the ***SPECTRUM Portable Management Application Tools Guide***:

- Charts, Graphs, and Meters
- Community Names
- Global Find MAC Address
- MIB I, II
- MIBTree
- Path
- Telnet
- TFTP Download
- Trap Table
- UPS

Charts, Graphs, and Meters are accessible from the Hub View and the command line; the Global MAC Address tool is accessible from the Hub View, the platform console window Tools menu, and the command line; the MIBTree application is available from the platform console window Tools menu, the Stand-alone Launcher applications menu, or the command line; and the rest of the tool applications (except Telnet) are available from the icon menu, the Hub View, or the command line. (The Telnet application is available only from the icon menu or the command line.)

Instructions on discovering Cabletron devices, creating icons, and accessing the icon menus within your management platform are included in your ***Installing and Using SPECTRUM for ...*** guide. If you are using SPMA for the 7C0x SmartSwitch in stand-alone mode — that is, without benefit of a specific network

management system — instructions for starting each application from the command line are included in each chapter of this guide and the ***SPMA Tools Guide***.

Conventions

SPECTRUM Portable Management Applications — including the 7C0x SmartSwitch module — can work with a number of different network management systems running on several different operating systems and graphical user interfaces. This versatility presents two documentation problems: first, there is no standard terminology; and second, the appearance of the windows will differ based on the graphical interface in use. For the sake of consistency, the following conventions will be followed throughout this and other SPMA guides.

Screen Displays

SPMA runs under a variety of different operating systems and graphical user interfaces. To maintain a consistent presentation, screen displays in this and other SPMA guides show an OSF/Motif environment. If you're used to a different GUI, don't worry; the differences are minor. Buttons, boxes, borders, and menus displayed on your screen may look a bit different from what you see in the guide, but they're organized and labelled the same, located in the same places, and perform the same functions in all screen environments.

Some windows within SPMA applications can be re-sized; those windows will display the standard window resizing handles employed by your windowing system. Re-sizing a window doesn't re-size the information in the window; it just changes the amount of information that can be displayed (see Figure 1-1). When you shrink a window, scroll bars will appear as necessary so that you can scroll to view all the information that is available.

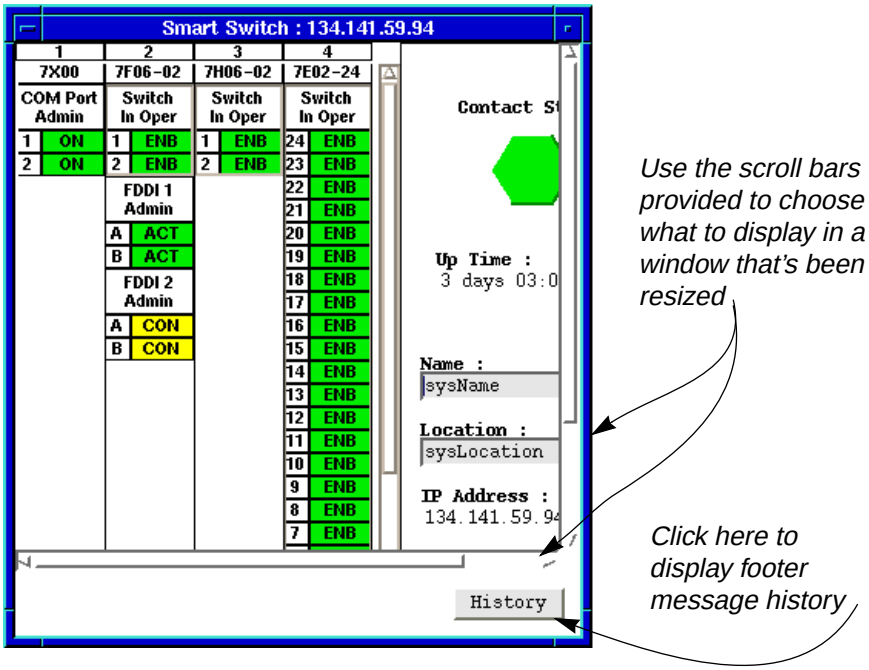


Figure 1-1. Window Conventions

Some windows will also contain a History button; selecting this button launches a History window (Figure 1-2) which lists all footer messages that have been displayed since the window was first invoked. This window can help you keep track of management actions you have taken since launching a management application.

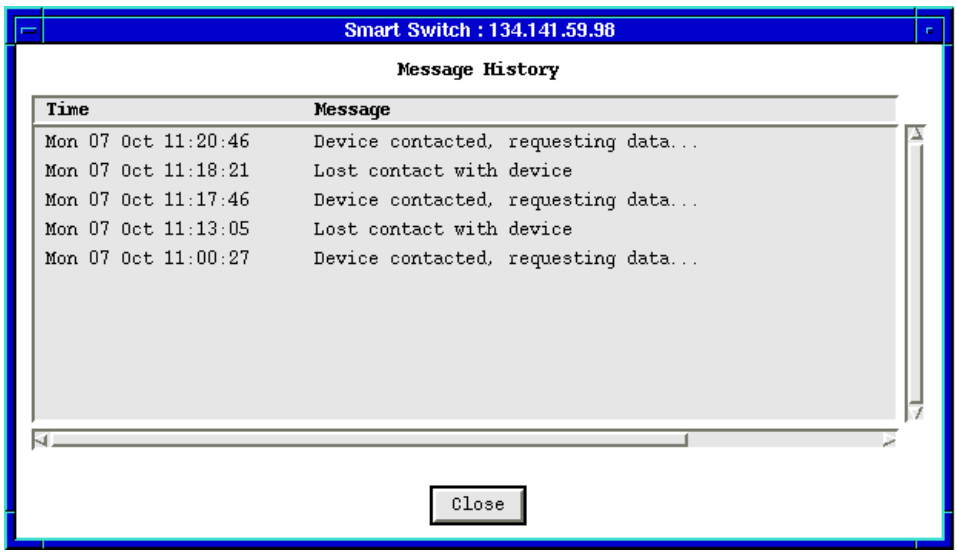


Figure 1-2. The History Window

Using the Mouse

The UNIX mouse has three buttons. Procedures within the SPMA document set refer to these buttons as follows:

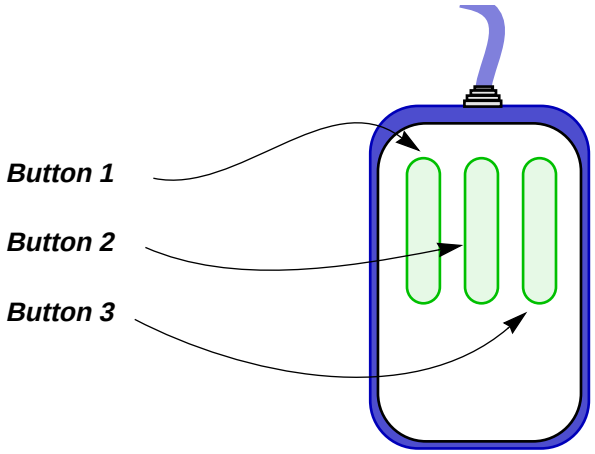


Figure 1-3. Mouse Buttons

If you're using a two-button mouse, don't worry. SPMA doesn't make use of mouse button 2. Just click the left button for button 1 and the right mouse button when instructed to use mouse button 3.

Whenever possible, we will instruct you on which mouse button to employ; however, menu buttons within SPMA applications will operate according to the convention employed by the active windowing system. By convention, menu buttons under the Motif windowing environment are activated by clicking the left mouse button (referred to as mouse button 1 in SPMA documentation), and there is no response to clicking the right button (mouse button 3). Under OpenWindows, menu buttons can be activated by clicking the right button, and convention dictates that the left button activates a default menu option; within SPMA, that default option will also display the entire menu. Because of this difference, references to activating a menu button will not include instructions about which mouse button to use. All other panels from which menus can be accessed, and all buttons which do not provide access to menus, will operate according to SPMA convention, as documented.

Getting Help

If you need additional support related to SPMA, or if you have any questions, comments, or suggestions related to this manual, contact Cabletron Systems Technical Support. Before calling, please have the following information ready:

- The product name and part number
- The version number of the applications that you need help with. SPMA is modular, which means each application will have a specific revision number. Where applicable, an INFO button provides the version number; you can also view the version number for any application by typing the command to start the application followed by a **-v**.

You can contact Cabletron Systems Technical Support by any of the following methods:

By phone:	Monday through Friday between 8 AM and 8 PM Eastern Standard Time at (603) 332-9400
By mail:	Cabletron Systems, Inc. PO Box 5005 Rochester, NH 03866-5005
By CompuServe®:	GO CTRON from any ! prompt
By Internet mail:	support@ctron.com
By FTP	ctron.com (134.141.197.25)
Login	`anonymous`
Password	`your email address`
By BBS:	(603) 335-3358
Modem Setting	8N1: 8 data bits, 1 stop bit, No parity

For additional information about Cabletron Systems products, visit our World Wide Web site: **http://www.cabletron.com/**

7C0x SmartSwitch Firmware

SPMA for the 7C0x SmartSwitch has been tested against released firmware version 1.02.05 and pre-release version 1.03.00 for the 7X00 Controller Module, and pre-release version 1.00.04 for the 7A06-01 NIM; if you have an earlier version of firmware and experience problems running SPMA, contact Cabletron Systems Technical Support for upgrade information.

NOTE

As a general rule, firmware versions for new products are liable to change rapidly; contact Cabletron Systems Technical support for information about the latest customer release of firmware available.

Chapter 2

Using the 7C0x SmartSwitch Hub View

Navigating through the Hub View; monitoring hub performance; managing the hub

The heart of the SPECTRUM Portable Management Application (SPMA) for the 7C0x SmartSwitch is the Hub View, a graphical interface that gives you access to many of the functions that provide control over the 7C0x hub and its installed modules.

Using the Hub View

There are two ways to open the Hub View: if you are working within a network management system, you can select the **Hub View** option from the icon menu; specific directions for creating a 7C0x SmartSwitch icon and accessing the icon menu can be found in the appropriate ***Installing and Using...*** guide. If you are running the 7C0x SmartSwitch module in a stand-alone mode, type the following at the command line:

```
spmarun fps <IP address> <community name>
```

The community name you use to start the module must have at least **Read** access; for full management functionality, you should use a community name that provides **Read/Write** or **Superuser** access. For more information on community names, consult the appropriate ***Installing and Using...*** guide, and/or the **Community Names** chapter in the ***SPMA Tools Guide***.

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from the icon menu or from within the Hub View.*

*If there is a hostname mapped to your 7C0x SmartSwitch's IP address, you can use **<hostname>** in place of **<IP address>** to launch the Hub View. Please note, however, that the hostname is **not** the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

Navigating Through the Hub View

Within the Hub View, you can click mouse buttons in different areas of the window to access various menus and initiate certain management tasks. The following sections describe the information displayed in the Hub View and show you how to use the mouse to manipulate the Hub View display.

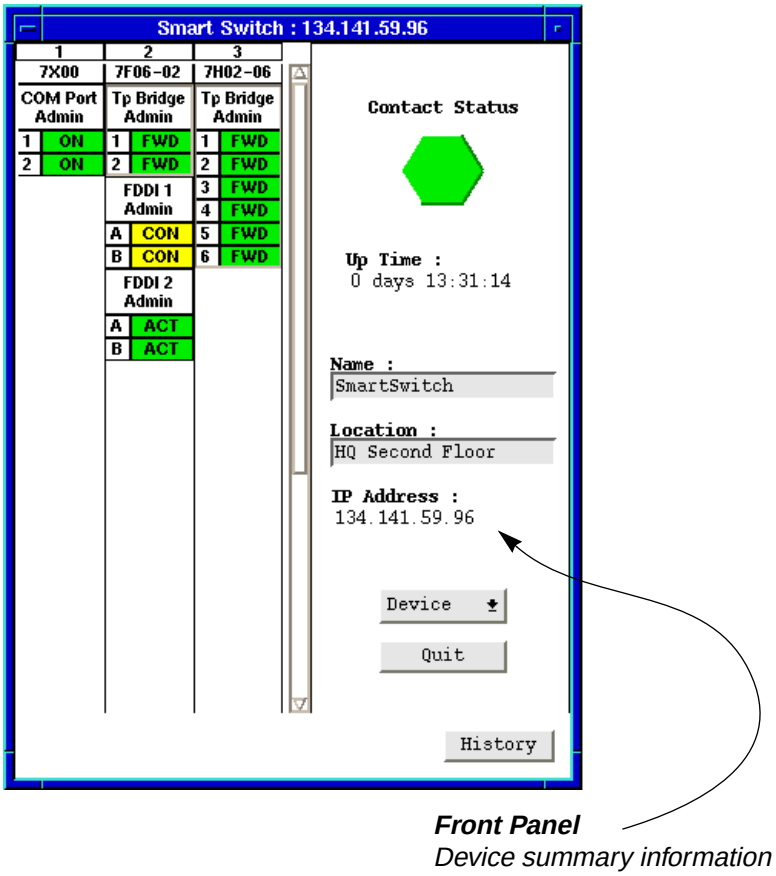


Figure 2-1. 7C0x SmartSwitch Hub View

Hub View Front Panel

In addition to the graphical display of the modules installed in your 7C0x SmartSwitch chassis, the Hub View gives you device level summary information. The following Front Panel information appears to the right of the module display:

Contact Status is a color code that shows the status of the connection between SPMA and the device:

- Green means a valid connection.
- Blue means that SPMA is trying to reach the device but doesn't yet know if the connection will be successful.
- Red means that SPMA is unable to contact or has lost contact with the device.

Uptime

The time that the device has been running without interruption. The counter resets to 00:00:00 (HH:MM:SS) when one of the following occurs:

- Power to the device is cycled.
- The device is reset manually.

Device Name

A text field that you can use to help identify the device; you can assign a device name via the MIB I, II application (described in the ***SPMA Tools Guide***). To view a name which is longer than the field, click to place your cursor in the text box, and use the arrow keys to shift the display.

Device Location

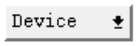
A text field that you can use to help identify the device; you can assign a device location via the MIB I, II application (described in the ***SPMA Tools Guide***). To view a location which is longer than the field, click to place your cursor in the text box, and use the arrow keys to shift the display.

NOTE

Although you can erase the current name and location and enter new values in the text fields, you cannot set these values from the Hub View. Any value you attempt to set will remain in the text field only until the Hub View is closed; to permanently change the name or location, you must do so via the MIB I, II application.

IP Address

The device's Internet Protocol address; this field will display the IP address you have used to create the 7C0x SmartSwitch icon (if you are running the Hub View from a management platform) or the IP address you used to launch the Hub View program (if you are running in stand-alone mode). You cannot change the 7C0x SmartSwitch's IP address from SPMA.



Clicking the **Device** button displays the Device menu, Figure 2-2.

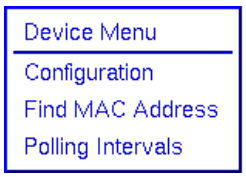
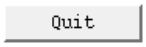


Figure 2-2. 7C0x SmartSwitch Hub View Device Menu

The Device menu lets you perform the following:

- Open the Device Configuration window
- Launch the Global Find MAC Address tool (described in the ***SPMA Tools Guide***)
- Open the Polling Intervals window

Note that the Device menu provides access to only a few of the applications which are available to the 7C0x SmartSwitch; additional applications are available from the Module, Switch, Bridge, Interface, and Port menus, and many can also be accessed both from the icon menu (if you are running under a network management platform) and from the command line (if you are running in stand-alone mode). See Chapter 1, **Introduction to SPMA for the 7C0x SmartSwitch**, for a complete list of applications available to the 7C0x SmartSwitch and how to access each one.



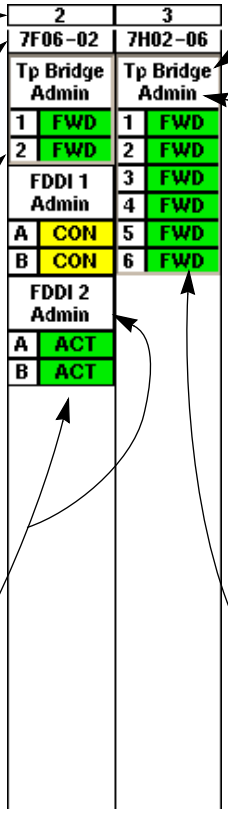
Clicking mouse button 1 on the **Quit** button closes all Hub View application windows; any open applications which can also be accessed from the command line or from the icon menu will remain open.

Using the Mouse in a Hub View Module

Each network interface module, or NIM, installed in the 7C0x SmartSwitch hub will be displayed in the hub view; use the mouse as indicated in the illustration below to access Module, Switch/Bridge/Interface, and Port menus and functions.

TIP

Note that slots 3 and 4 of the 7C04-R chassis can accept either the double-wide NIM modules or the standard-size modules; both module types display as the same size in the Hub View.



Module Index
Indicates the module's slot number within the 7C0x hub. (Slots are numbered from left to right; the controller module slot is slot #1.) Click button 1 or button 3 to display the Module menu.

Module Type
Indicates the module's type. Click button 1 or button 3 to display the Module menu.

Port Index
Click button 1 to toggle the interface between enabled and disabled; click button 3 to display the Port menu (bridge display mode only).

FDDI Front Panel Status
For FDDI modules only, a separate Front Panel display shows the status of the individual A and B ports that together form a single interface. Click either button to access the FDDI menu.

Display Mode
Indicates the Display Mode currently in effect; available modes are Switch or Bridge, Interface, and None. Click either mouse button to display the Switch, Bridge, or Interface menu; both the menu that appears and the status displays will vary based on the mode selected.

Port Display Form
Using the Bridge, Switch, Interface, or FDDI menus, you can change the information displayed in each port status box; available options vary according to menu.

Port Status
The Port Status display changes with the type of port display format selected. Click button 1 to toggle the interface between enabled and disabled; click button 3 to display the Port menu (bridge display mode only).

Figure 2-3. Mousing Around a Module Display

Monitoring Hub Performance

The information displayed in the Hub View can give you a quick summary of device activity, status, and configuration. SPMA can also provide further details about hub performance via its multi-level menu structure: first, you select the hub view display mode for the services you want to monitor (Switch, Bridge, or Interface); then, you can use the available menus (Figure 2-4, below) to access the tools that let you monitor specific aspects of hub performance and set 7C0x SmartSwitch operating and notification parameters.

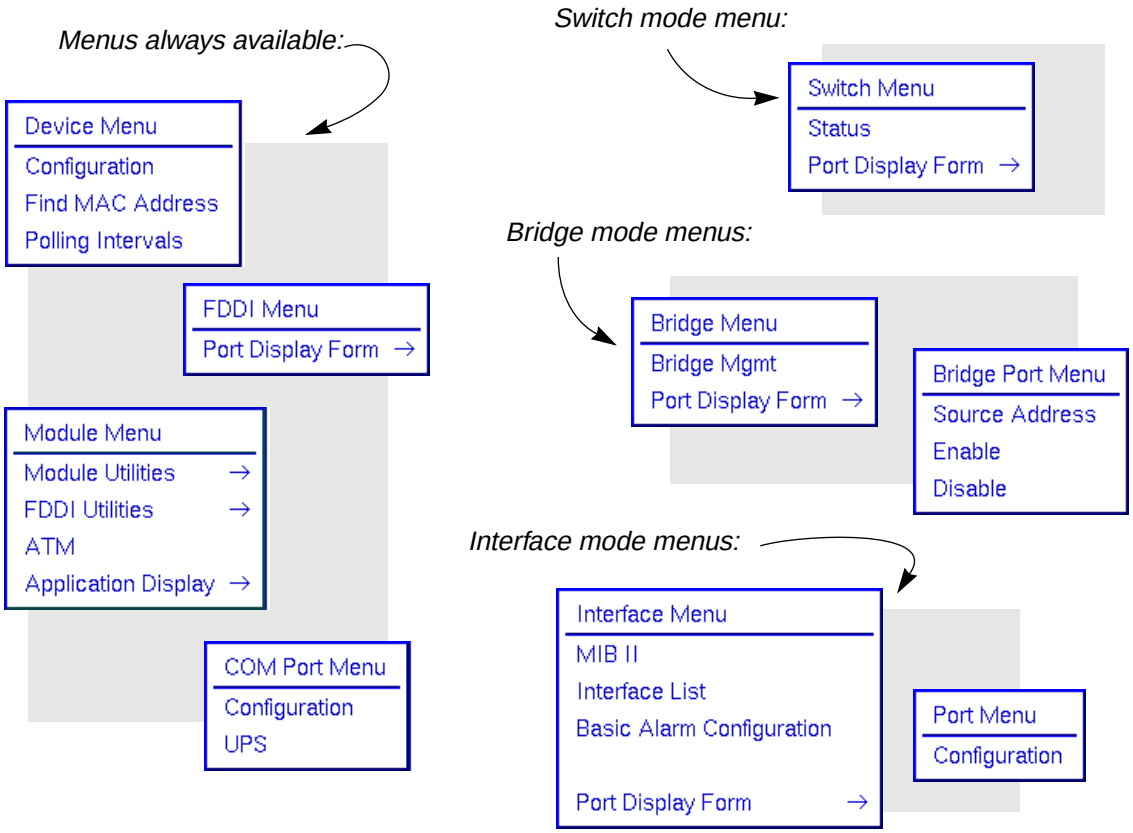


Figure 2-4. The 7C0x SmartSwitch's Device, Module, Switch, Bridge, Interface, FDDI, and Port Menus

Selecting the Application Display Mode

The device information, menus, and applications that are available to you via the Hub View depend on the Application Display mode you have chosen. For the 7C0x, you can select from a total of four Application Display modes:

- **Switch**, which displays switching status in the port displays, and provides menu access to switch management applications; note that this option is only available for devices configured to operate in switch mode.
- **Bridge**, which displays bridging status in the port displays, and provides menu access to bridge management; note that this option is only available for devices configured to operate in bridge mode.
- **Interface**, which displays each port's MIB II status and statistics.
- **None**, which removes all interface status information from the Hub View. This selection primarily effects FDDI modules, whose front panel A and B ports will continue to display their individual status; Ethernet, Fast Ethernet, and ATM modules will display as blank under this mode.

You select the Application Display mode you want via the Module menu (Figure 2-5); note that the Module menu remains the same regardless of which display mode is selected.

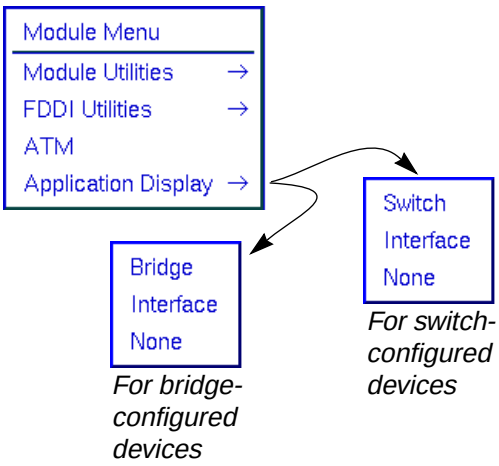


Figure 2-5. The Hub View Module Menu

TIP

Note that, although the Module menu does not change based on the Application Display mode selected, the ATM option will only appear when a 7A06-01 NIM is installed in the chassis. See ***Accessing ATM Management****, page 2-28, for more information.*

By default, the 7C0x Hub View will launch in Switch display mode (for those devices configured via Local Management to perform SecureFast switching) or Bridge display mode (for those configured to perform traditional bridging); to change this:

1. Click mouse button 1 or mouse button 3 in the Module Index or Module Type display boxes in the Hub View (see Figure 2-3, page 2-5) to display the Module menu.

2. Drag down to **Application Display**, then across to select the display mode you want. Note that only three selections are available at any one time: either **Bridge** or **Switch** (depending on the device's current configuration), **Interface**, and **None**.

When you change the application display mode, the port display form will change to the default form for the chosen mode; you can change the port display form and access various management applications via each mode's menu structure, as described in the following sections.

COM Port and FDDI Front Panel Displays

Note that, like the Module menu, neither the COM port nor the FDDI front panel displays are affected by changes in the Application Display. The COM port display always shows each port's administrative status (ON or OFF), both in the text display and in the color code (green = ON, blue = OFF); the FDDI front panel display changes based on the port display form selected via the FDDI menu, as illustrated below.

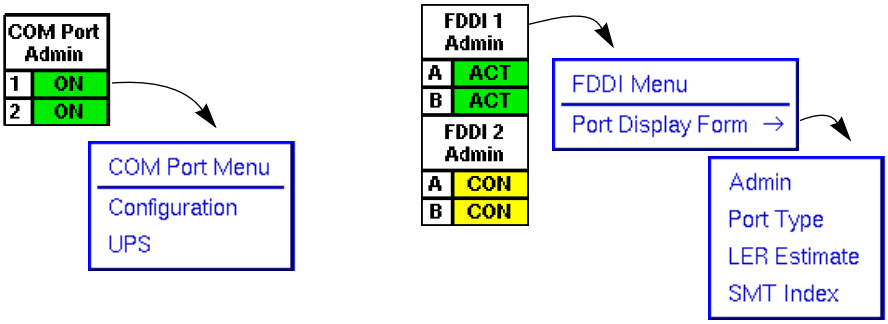


Figure 2-6. COM Port and FDDI Front Panel Displays

Both the FDDI and COM port menus are available and display the same options in all Application Display modes.

TIP

Note that, although the COM port menu does not change based on the Application Display mode selected, the UPS option will only appear for COM ports which have been configured for a UPS. See ***Configuring COM Ports****, page 2-36, for more information.*

FDDI Port Display Forms

You can display the following information in the front panel port displays for any installed FDDI NIM:

Admin

Displays the connection state of each port:

- **CON** (connecting) — the port is trying to establish a link, but has not yet been successful. Ports which are not connected and which have not been disabled by management will display this status.
- **ACT** (active) — the port has been enabled by management and has successfully established a link.
- **SBY** (standby) — the port has a physical link, but the SMT Connection Policy is prohibiting a logical connection to the ring because the attempted connection is illegal. FDDI protocol always forbids connecting two Master ports; all other connections are theoretically legal, although some are not

desirable. You can view and configure the SMT Connection Policy by selecting the **SMT Connection Policy** option on the Module —>FDDI Utilities menu; see Chapter 4, **FDDI Management**, for more information.

- **DIS** (disabled) — the port has been disabled by management; note that this status does not indicate whether or not there is a physical link connected to the port.

Port Type

Displays the media type of each A and B port:

- MMF (multi-mode fiber)
- SMF (single-mode fiber)
- SON (SONET)
- LCF (low-cost fiber)
- TP (twisted pair)

LER Estimate

The Link Error Rate (LER) Estimate port display form displays a cumulative long-term average of the bit error rate, which represents the quality of the physical link. It is computed when the port is connected and every 10 seconds thereafter. The value of the LER Estimate can range from 10^{-4} to 10^{-15}, but is always displayed as the absolute value of the exponent: for example, if the port's LER Estimate is computed to be 10^{-5}, the value displayed in the Port Status box will be 5, which represents an actual rate of 1,250 bit errors per second. The lower LER Estimate numbers represent the highest bit error rates, as summarized in the figure below:

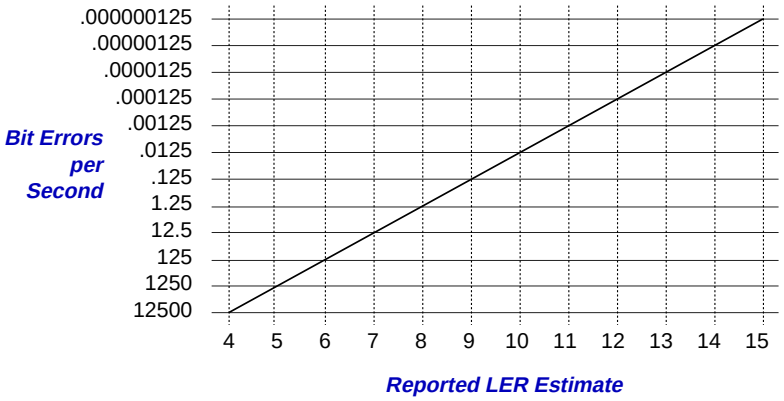


Figure 2-7. LER Estimate Values

TIP

*You can configure alarm thresholds for the LER Estimate; see Chapter 4, **FDDI Management**, for more information.*

SMT Index

Displays each port's *logical* index number, which reflects the port's logical position in relation to the SMT entity to which it is assigned. (Each FDDI interface has its own SMT entity; these are indexed from left to right in the hub, and from top to bottom on each module.) Note that the assigned *logical* index numbers do not necessarily reflect each port's *physical* position on the module or in the hub; for example, an interface whose physical index is 20002 might have individual A and B logical indices of 1.1 and 1.2, indicating that the A and B ports which together form the interface are ports number 1 and 2 assigned to SMT number 1.

TIP

For more information on all of these FDDI states, see Chapter 4, ***FDDI Management****.*

FDDI Color Codes

For all FDDI port display forms, the color coding is the same:

- **Green** indicates that the port is active; this is, the port has been enabled by management, has a valid Link signal, and is able to communicate with the station at the other end of the port's cable segment.
- **Blue** indicates that the port has been disabled through management, or that it is in a standby state.
- **Yellow** indicates that the port is enabled but does not currently have a valid connection. This usually indicates that the device at the other end of the segment is turned off, or that no cable segment is attached.
- **Red** indicates that port is administratively enabled, but not operational due to some hardware or network problem.

The Switch Application Display

The Switch Application Display — available only for devices which have been configured (via Local Management) to operate as SecureFast switches — allows you to view each switch interface according to switching status and statistics; it also provides access to the Switch menu (Figure 2-8), from which you can launch a Switch Status window and change the port display form. This is the default display mode for devices configured for SecureFast operation.

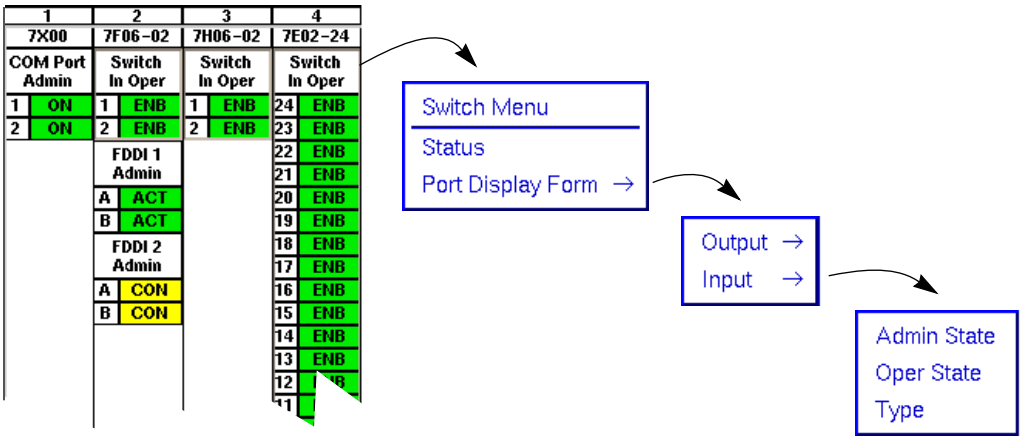


Figure 2-8. The Switch Application Display and Menu

For more information about the Switch Status window, see **Viewing Switch Status**, page 2-23; port display forms are described below.

Switch Port Display Forms

You can select three port display forms for switch interfaces; note that, although you can select both Input and Output state for each interface, it is unlikely that any single interface would have different input and output status values at any given time.

Admin State

An interface's Administrative State is the state currently *requested* by management; note that this may not always be the same as the *actual*, or Operational, state described below:

- **ENB** (enabled) — the port is administratively enabled.
- **DIS** (disabled) — the port is administratively disabled.

Oper State

An interface's Operational State is its *actual* state; note that this may not always be the same as the *requested*, or Admin, state described above:

- **ENB** (enabled) — the port is enabled.
- **DIS** (disabled) — the port is disabled.
- **PDIS** (pending disable) — the port is in a transitional state, moving toward a state of disabled.
- **PENB** (pending enable) — the port is in a transitional state, moving toward a state of enabled.

- **INV** (invalid configuration) — the port is in an unrecognized state.
- **TST** (testing) — the port is in a testing mode.

Type

A switch interface's Type is a dynamic value determined by the type of node to which the interface is connected:

- **Ntwk** (network) — a Network interface is connected to another switch.
- **Access** — an Access interface is connected to an end node (a single user, a shared resources such as a server or print, or a non-switch shared access interface such as a bridge).
- **Hybrid** — though this feature is not yet supported, future firmware versions will allow a switch interface to service both another switch and an end node. This kind of configuration could occur, for example, on an FDDI ring.
- **GoAcc** (going to access) — a transitional state experienced by an interface which is in the process of switching to access mode.
- **Unkn** (unknown) — on boot-up, all switch interfaces have a type value of unknown; this value will convert dynamically as required by the connected node.

Switch Port Color Codes

The color codes assigned to each port interface in Switch Application mode indicate the following status conditions:

- **Red** — the port is administratively enabled, but not operational. This state generally indicates that a network problem has shut down the port, even though it is still administratively enabled; it can also indicate an invalid port configuration.
- **Blue** — the port is both administratively and operationally disabled.
- **Green** — the port is administratively enabled and operational.
- **Yellow** — the port is in a transitional state: an operational status of either enable or disable is pending, or the port has been administratively disabled, but is (temporarily) still operational.
- **Magenta** — the port is in a transitional testing mode.

Note that the color coding scheme is the same regardless of the port display form selected.

The Bridge Application Display

The Bridge Application Display — available only for devices which have been configured (via Local Management) to operate as traditional bridges — allows you to view each bridge interface according to bridging status and statistics; it also provides access to the Bridge and Bridge Port menus (Figure 2-9), from which you can launch the Bridge View application, change the port display form, view a list of source addresses communicating through a selected interface, and enable or disable a selected interface. This is the default display mode for devices configured for traditional bridging.

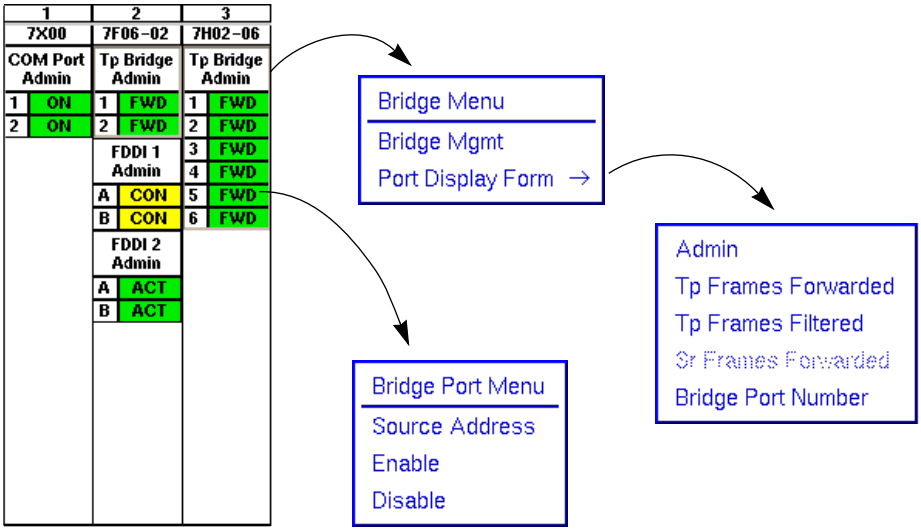


Figure 2-9. The Bridge Application Display and Menus

For more information about the Bridge View application, see Chapter 6, **Using the 7C0x Bridge View**; for more information about viewing source addresses, see **Viewing the Source Address List**, page 2-24; and for more information on enabling and disabling a bridge interface, see **Enabling and Disabling Bridge Ports**, page 2-38. Port display forms are described below.

Bridge Port Display Forms

You can display the following information for each bridging interface:

Admin

Displays the port's current bridging status:

- **FWD** (forwarding) — the port is on-line and ready to forward packets from one network segment to another. Note that this is the default display for ports which are administratively enabled but not connected.

- **DIS** (disabled) — the port has been disabled by management; no traffic can be received or forwarded on this port, including configuration information for the bridged topology.
- **LIS** (listening) — the port is not adding information to the filtering database; it is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move to the forwarding state.
- **LRN** (learning) — the filtering database is being created, or the Spanning Tree Algorithm is being executed because of a network topology change. The port is monitoring network traffic, learning network addresses.
- **BLK** (blocking) — the port is on-line, but filtering traffic from going across the 7C0x SmartSwitch from one network segment to another. Bridge topology information is still being forwarded.
- **BRK** (broken) — the physical interface has malfunctioned.

Tp Frames Forwarded

Displays the percentage of total frames received that were transparently forwarded across the selected interface.

Tp Frames Filtered

Displays the percentage of total frames received that were filtered at the selected interface.

Sr Frames Forwarded

Displays the rate at which source route frames are being forwarded across the selected interface, in a frames/second format. Note that this option is currently grayed out, as no Token Ring NIMs are yet available.

Bridge Port Number

Displays the index number assigned to each bridge port interface. Bridge ports are indexed from left to right by module, beginning with the module installed in slot 2; on each module, bridge port numbering follows the physical port indexing. For example, the port display illustration in Figure 2-9 (page 2-13) contains eight bridge interfaces: the two interfaces on the FDDI module installed in slot 2 are bridge port numbers 1 and 2 (corresponding to physical ports 1 and 2); the six interfaces on the Fast Ethernet module installed in slot 3 are bridge ports 3 through 8 (corresponding to physical ports 1 through 6).

NOTE

You will note that some Ethernet modules display an upside-down port indexing, with the highest index numbers at the top of the module, and the lowest ones at the bottom; for these modules, the bridge port numbers will still follow the physical port indexing, with the higher bridge port numbers corresponding to the higher physical port indices.

Bridge Port Color Codes

The color codes assigned to each port interface in Bridge Application mode indicate the following bridging status conditions; note that the color coding is the same for all port display forms:

- **Green —** the port is in a Forwarding state; that is, it is on-line and ready to forward packets from one network segment to another. Note that this is the default display for ports which are administratively enabled but not connected.
- **Blue —** the port has been disabled by management; no traffic can be received or forwarded on this port, including configuration information for the bridged topology.
- **Magenta —** the port is in a Listening or Learning state.
- **Orange —** the port is on-line, but filtering (blocking) traffic from going across the 7C0x SmartSwitch from one network segment to another. Bridge topology information is still being forwarded.
- **Red** — the physical interface has malfunctioned (the port is broken).

The Interface Application Display

The Interface Application Display mode allows you to view the interfaces on all installed modules according to MIB II status and statistics; it also provides access to the Interface and Interface Port menus (Figure 2-10), from which you can launch the MIB I, II application, view the interface list, configure alarms, perform any available port configuration, and, of course, change the port display form.

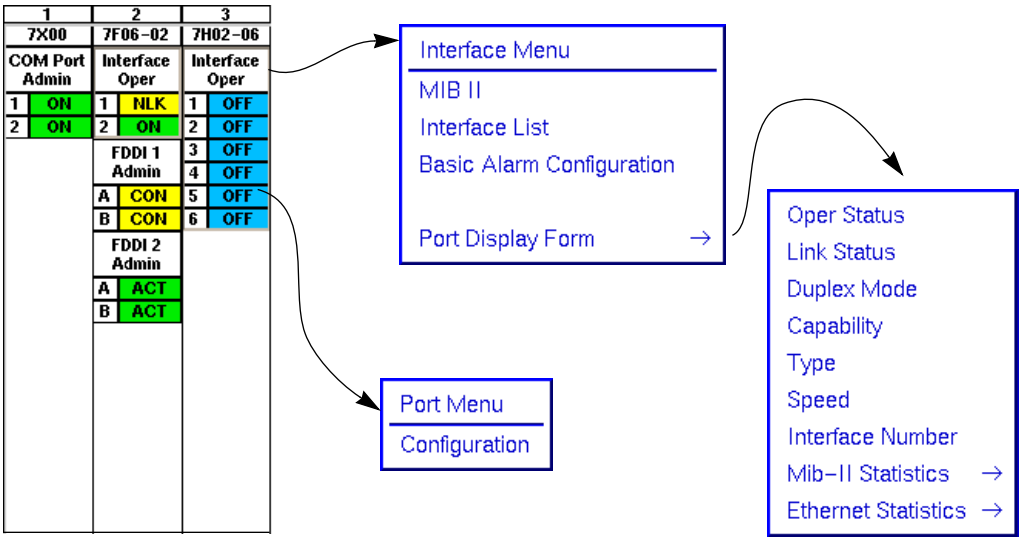


Figure 2-10. The Interface Application Display and Menus

For more information about the MIB I, II application, see the ***SPMA Tools Guide***; for more information about the interface list, see **Viewing the Interface List**, page 2-22; for more information about configuring alarms, see Chapter 3, **Alarm Configuration**; and for more information about available port configuration options, see **Port Configuration**, page 2-30; port display forms are described below.

Interface Port Display Forms

You can display the following information for each available interface:

Oper Status

An interface's Operational Status is its *actual* state; note that this may not always be the same as the *requested*, or administrative state:

- **ON** — the port is administratively enabled, a link is present, and the port is functioning normally.
- **NLK** (no link) — the port is administratively enabled, but no link is present. This typically indicates that no cable is currently connected to the interface.
- **OFF** — the port is not operational; this may be because it has been administratively disabled, it has malfunctioned in some way, or it is attempting to move into a testing state. Note that the color code (described in the following section, page 2-20) that accompanies this display will indicate which of these three conditions has caused the OFF state.
- **TEST** — the port is being tested.

Link Status

A port's Link Status tells you whether or not the port has a valid connection to the node at the other end of the cable segment. Note that this status does not provide any indication of administrative (ON or OFF) or operational status.

- **NLK** (no link) — no link is present.
- **LNK** — a link is present.

Duplex Mode

The Duplex Mode status indicates which interfaces have been configured to operate in Full Duplex mode, and which are operating in standard mode. Interfaces which are operating in full duplex mode can both transmit and receive packets at the same time, effectively doubling the wire speed; interfaces in standard mode must finish transmitting before they can receive, and vice versa.

- **Stand** — the interface is operating in standard mode.
- **Full** — the interface is operating in full duplex mode.

Capability

The Capability display indicates the highest duplex mode of which the interface is capable. Note that this display does not indicate the current Duplex Mode setting.

- **Full** — the interface can be configured to operate in Full Duplex mode.
- **Fast** — the interface is a Fast Ethernet port, and can be configured to operate in Full Duplex mode. Note that, for a Fast Ethernet port, Full Duplex operation doubles wire speed from 100 Mbps to 200.
- **Stand** — the interface can operate only in standard mode.

Type

The Type display indicates each interface's topology type:

- **Eth** — Ethernet or Fast Ethernet
- **FDDI**
- **ATM**

Speed

This display indicates the defined wire speed for each interface's topology. Note that this speed value does not indicate whether or not a selected port is operating in Full Duplex mode (which effectively doubles the defined wire speed). Possible values are:

- **10M** — 10 megabits per second, for standard Ethernet
- **100M** — 100 megabits per second, for Fast Ethernet, FDDI, and ATM

Interface Number

Displays the index number assigned to each interface. Index numbers are assigned in an XXXXYY format, where X = slot index times 10,000, and Y = port index. For example, an interface index of 30017 would be assigned to port 17 on the module installed in slot 3 of the chassis.

MIB II Statistics

You can use the MIB II Statistics options to view selected statistics for each port as a percentage of the total traffic seen on that interface.

- **Load** — shows a value for each active port that represents that port's traffic as a percentage of the theoretical maximum load. You can view the load in three ways:
  - **In** — indicates the number of inbound packets as percentage of the theoretical maximum load.
  - **Out** — indicates the number of outbound packets as a percentage of the theoretical maximum load.
  - **Total** — indicates the total number of inbound and outbound packets as a percentage of the theoretical maximum load.

For Ethernet ports, the theoretical maximum load is 10 Mbps; for Fast Ethernet, FDDI, and ATM, it's 100 Mbps.

- **Discard** — shows a value for each active port that indicates what percentage of the total packets received at or transmitted by that port were discarded. You can view the discard percentage in three ways:
  - **In** — indicates the number of inbound packets that were discarded, as a percentage of the total load experienced by that port.
  - **Out** — indicates the number of outbound packets that were discarded, as a percentage of the total load experienced by that port.
  - **Total** — indicate the total number of packets that were discarded, as a percentage of total load.
- **Errors** — shows a value for each active port that indicates what percentage of the total packets received at or transmitted by that port contained an error. You can view the error percentage in three ways:
  - **In** — indicates the number of inbound packets that contained errors, as a percentage of the total load experienced by that port.
  - **Out** — indicates the number of outbound packets that contained errors, as a percentage of the total load experienced by that port.
  - **Total** — indicate the total number of packets that contained errors, as a percentage of total load.
- **Nucast** (non-unicast) — shows a value for each active port that indicates what percentage of the total packets received at or transmitted by that port were non-unicast (that is, broadcast or multicast) packets. You can view the non-unicast percentage in three ways:
  - **In** — indicates the number of inbound packets that were broadcast or multicast packets, as a percentage of the total load experienced by that port.
  - **Out** — indicates the number of outbound packets that were broadcast or multicast packets, as a percentage of the total load experienced by that port.
  - **Total** — indicate the total number of broadcast and multicast packets, as a percentage of total load.

Ethernet Statistics

For any Ethernet or Fast Ethernet modules installed in your SmartSwitch chassis, you can view a variety of RMON statistics as a percentage of the total load experienced by each port. Note that this option will only be available when at least one Ethernet or Fast Ethernet module is installed in the chassis; when one of these options is selected, the port displays for any installed FDDI or ATM modules will display three dashes (---). Ethernet statistical selections available are:

- **Load** — shows a value for each active port that represents that port's traffic as a percentage of the theoretical maximum load: either 10 Mbps (for Ethernet), or 100 Mbps (for Fast Ethernet).
- **Packets** — displays the number of good packets experienced by each interface in one of four ways:
  - **Packets/second** — the rate of traffic being experienced by the port
  - **Average Packet Size** — displayed in bytes; calculated by dividing the total number of octets by the total number of good packets
  - **Broadcast** — the percentage of good packets on each port that are broadcast packets
  - **Multicast** — the percentage of good packets on each port that are multicast packets
- **Collisions** — displays the total number of *receive* (those the device detects while receiving a transmission) and *transmit* (those the device detects while transmitting) collisions, as a percentage of the total traffic experienced by the port.
- **Errors** — displays the total number of packets with a specific error type, as a percentage of the total number of *errors* experienced by the port. Available error types are:
  - **CRC/Alignment** — the number of packets processed by a port that had a non-integral number of bytes (alignment errors) or a bad frame check sequence (Cyclic Redundancy Check, or CRC error), expressed as a percentage of the total number of error packets experienced by the port.
  - **Fragments** — the number of packets processed by a port that were undersized (less than 64 bytes in length; a **runt** packet) ***and*** had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error), expressed as a percentage of the total number of error packets experienced by the port.
  - **Jabbers** — the number of packets processed by a port that were oversized (greater than 1518 bytes; a **giant** packet) ***and*** had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error), expressed as a percentage of the total number of error packets experienced by the port.
- **Frame Sizes** — displays the total number of packets processed by a port that were of a specific size, expressed as a percentage of the total number of good packets experienced by the port. Frame size breakdowns available are:
  - **Runts** (packets with fewer than 64 bytes)
  - **64**
  - **65-127**
  - **128-255**
  - **256-511**

- **512-1023**
- **1024-1518**
- **Giants** (packets with more than 1518 bytes)

NOTE

Note that, for all statistical port display form options (both MIB II and Ethernet), three dashes (---) will display for all inactive ports; any active (green) port will display a numeric value, even if it's zero. In addition, any FDDI or ATM interface will display three dashes for any Ethernet statistical display selection.

Interface Port Color Codes

The color codes assigned to each port interface in the Interface Application Display mode indicate a combination of administrative (desired) and operational (actual) status; note that the color coding is the same for all port display forms:

- **Green** — the port is administratively enabled, linked, and operating normally.
- **Yellow** — the port is administratively enabled, but no link is present.
- **Red** — the port is administratively enabled, but not operational; this generally indicates some kind of malfunction.
- **Blue** — the port is administratively disabled, and is not operational. Note that this state does not indicate link status.
- **Magenta** — indicates either that a testing mode has been requested but is not yet in effect, or that testing is taking place.

Viewing Device Configuration

If you need to call Cabletron's Technical Support about a problem with the Hub View application or your 7C0x SmartSwitch hardware, you'll need the information provided in the Device Configuration window. To launch the window:

1. Click on Device to display the Device menu; note that this menu is the same regardless of the Application Display mode currently in effect.
2. Drag down to **Configuration**, and release. The Device Configuration window, Figure 2-11, will appear.

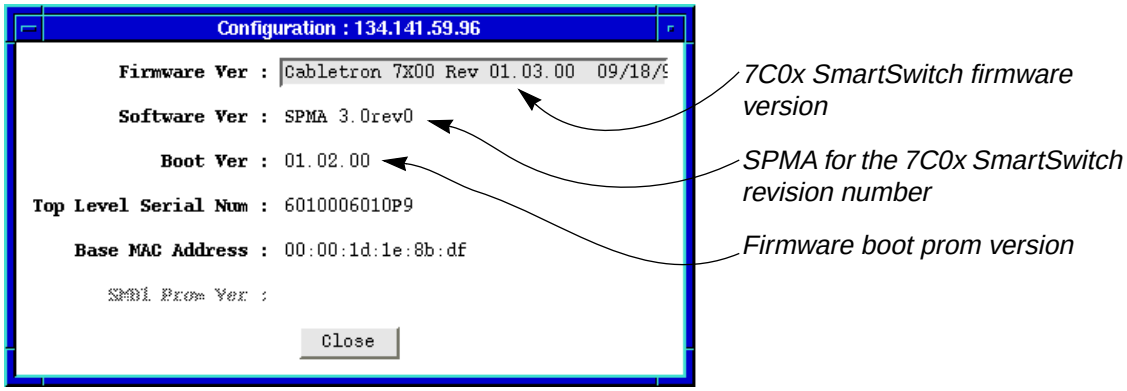


Figure 2-11. Device Configuration Window

The Device Configuration window provides the following hardware and software revision information:

Firmware Version

Displays version information for the firmware currently installed on your 7X00 controller module. To view a truncated description, click to place your cursor in the text field, then use the arrow keys to shift the display.

NOTE

Although the text field allows you to edit and/or delete the displayed firmware description, you cannot set any changes you make. The information appears in a text field only so that it will be scrollable, allowing you to view the complete description.

Software Version

Displays the version of the SPMA Hub View application for the 7C0x SmartSwitch.

Boot Version

Displays the revision level of the 7X00 controller module's boot prom.

Top Level Serial Number

Displays the serial number assigned to the 7X00 controller module. This serial number contains information about the date and location of manufacture, and the hardware revision level.

Base MAC Address

Displays the MAC address of the 7X00 controller module's Host interface — the interface that connects to the 7C0x hub's switching backplane.

Viewing the Interface List

You can use the Interface List application to view a complete list of MAC Addresses assigned to the interfaces installed in your 7C0x SmartSwitch chassis.

To open the Interface List:

1. If necessary, put the Hub View into the Interface Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then across to select **Interface**).

2. Click either mouse button on the Display Mode box in the Hub View to launch the Interface menu; drag down to **Interface List**, and release. The Interface List window, Figure 2-12, will appear.

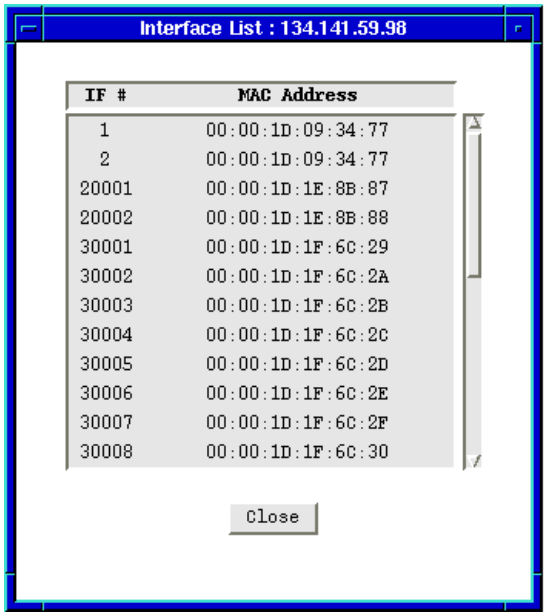


Figure 2-12. Interface List Window

The Interface List window displays an **IF #** for each interface and the **MAC Address** (physical address) associated with each interface. The first two interfaces are the 7X00 controller module's interfaces to the 7C0x chassis switching backplane; note that they share a MAC address. The remaining index numbers are assigned in an XXXXYY format, where X = slot index times 10,000, and Y = port index. For example, an interface index of 30017 would be assigned to port 17 on the module installed in slot 3 of the chassis.

The interface and MAC address information displayed here is taken directly from the MIB II Interface Table; you can view both the MAC address and the IF index via the Interface Protocol Status window available in the MIB I, II tool. For more information on the MIB I, II tool and the Interface Protocol Status window, refer to **Chapter 2** in the ***SPMA Tools Guide***.

Viewing Switch Status

For devices which have been configured to operate as SecureFast switches, you can view a Switch Status window (Figure 2-13) which provides general information about current switching operations.

To launch the Switch Status window:

1. If necessary, put the Hub View into the Switch Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then across to select **Switch**).
2. Click either mouse button on the Display Mode box in the Hub View to launch the Switch menu; drag down to **Status**, and release. The Switch Status window, Figure 2-13, will appear.

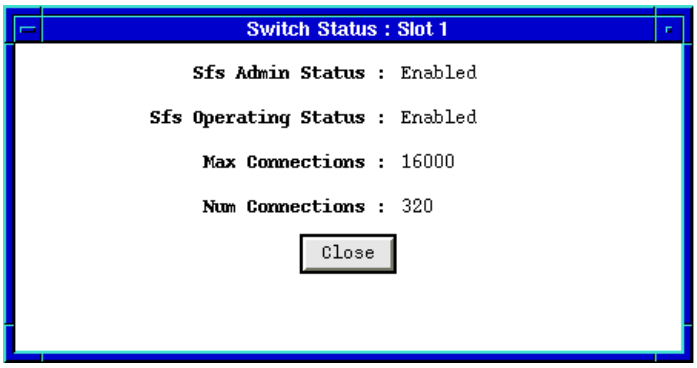


Figure 2-13. Switch Status Window

The Switch Status window provides the following general information about your SmartSwitch's SecureFast switch operation:

Sfs Admin Status

Displays the *requested* administrative status of the 7C0x's SecureFast switching services: **Enabled** or **Disabled**. Note that this may not always match the *actual*, or operating status, described below.

Sfs Operating Status
Displays the *actual* operational status of the 7C0x's SecureFast switching services: **Enabled**, **Disabled**, **Pending Enable** (start-up in progress), **Pending Disable** (shut-down in progress), or **Invalid Configuration**. Note that the *actual* operational status may not always match the *requested* administrative status described above.

TIP

For more information about administrative and operational states as they apply to individual switch interfaces, see ***Switch Port Display Forms***, *page 2-11*.

Max Connections
Displays the maximum number entries allowed in the Connection Table. Up to 16000 entries can be stored in the SmartSwitch's Connection Table.

Num Connections
Displays the number of entries currently stored in the Connection Table.

Viewing the Source Address List

For devices which have been configured to operate in traditional bridging mode, you can use the Source Addresses option available from the Bridge Port menu to view a list of all the MAC addresses that are communicating through a selected bridge interface.

To open the Source Addresses window:

1. If necessary, put the Hub View into the Bridge Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then across to select **Bridge**).
2. Click mouse button 3 on the Port Index or Port Status display for the bridge port whose source address list you wish to view; drag down to **Source Address**, and release. The Source Address window, Figure 2-14, will appear.

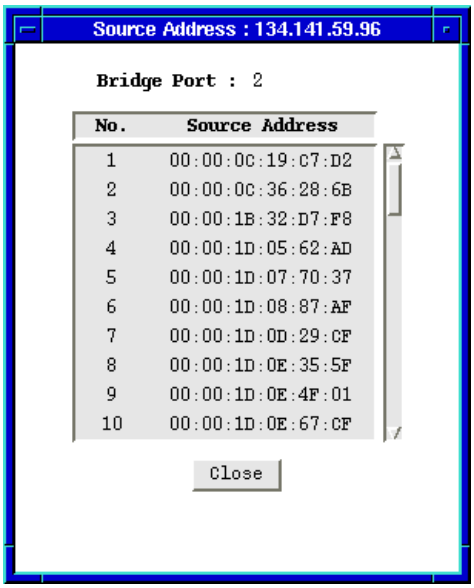


Figure 2-14. The Bridge Port Source Address Window

The bridge port Source Address window displays the MAC address of each device that has transmitted packets that have been forwarded through the selected bridging interface during the last cycle of the Filtering Database's defined ageing timer (learned addresses that have not transmitted a packet during one complete cycle of the ageing timer are purged from the Source Address Table). For more information on the Filtering Database, see in Chapter 6, **Using the 7C0x SmartSwitch Bridge View**.

Managing the Hub

In addition to the performance information described in the preceding sections, the Hub View also provides you with the tools you need to configure your hub and keep it operating properly. Hub management functions include setting polling intervals; launching a variety of SPMA Tool applications (including FDDI management applications, and the Bridge View application); performing all available port configuration for Ethernet, FDDI, Fast Ethernet, and COM ports; and enabling and disabling bridge ports.

Launching SPMA Tools from the Hub View

The 7C0x SmartSwitch Hub View provides access to most of the SPMA Tool applications available for your SmartSwitch. These tool applications are also available from the icon menu and the command line; they are described in detail in the ***SPMA Tools Guide***.

Module Utilities

Most of the available SPMA Tools can be launched from the **Module —> Module Utilities** menu. (Remember, the Module menu is available in any Application Display mode.) To launch a utility from this menu:

1. Click either mouse button on the Module Index or Module Type box in the Hub View to display the Module menu.
2. Drag down to **Module Utilities**, then across to select the tool you want to launch:
   a. **Community Names** (described in Chapter 3 of the ***SPMA Tools Guide***)
   b. **TFTP Download** (described in Chapter 5 of the ***SPMA Tools Guide***)
   c. **Trap Table** (described in Chapter 6 of the ***SPMA Tools Guide***)
   d. **Path Tool** (described in Chapter 10 of the ***SPMA Tools Guide***)

TIP

*One tool available for the 7C0x SmartSwitch but not accessible from within the Hub View is the **Telnet** application; this application provides remote access to Local Management, from which you can perform many basic configuration options — including selecting either SecureFast switching or traditional bridging.*

For more information about the Telnet application, see Chapter 4 of the **SPMA Tools Guide***; for more information about Local Management and the configuration options available there, consult the Local Management documentation shipped with your device.*

MIB I, II

The MIB I, II tool — which gives you direct access to the MIB II information stored in your 7C0x's MIB — is also available from within the Hub View. To launch it:

1. If necessary, put the Hub View into the Interface Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then across to select **Interface**).
2. Click either mouse button on the Display Mode box in the Hub View to launch the Interface menu; drag down to **MIB II**, and release.

The MIB I, II tool is described in detail in Chapter 2 of the ***SPMA Tools Guide***.

Find MAC Address

The newest member of the family of SPMA Tool applications, the Global Find MAC Address tool gives you the ability to locate the hub interface through which a specific MAC address is communicating. If you are running SPMA from within a network management platform (HP Network Node Manager, IBM NetView, or SunNet Manager), launching this tool from the platform's Console window Tools

menu allows you to search for a specified MAC address on multiple devices simultaneously; however, if you launch this tool from the Hub View or from the command line, only the hub against which you launch the tool will be searched.

To launch the Global Find MAC Address tool from the Hub View:

1. Click on Device to display the Device menu; note that this menu is the same regardless of the Application Display mode currently in effect.
2. Drag down to **Find MAC Address**, and release.

The Global Find MAC Address tool is described in detail in Chapter 12 of the ***SPMA Tools Guide***.

UPS

If either of the COM Ports on the 7X00 controller module has been configured for UPS operation (see **Configuring COM Ports**, page 2-36), that port's menu will include a selection that allows you to launch the UPS configuration tool.

To do so:

1. Click either mouse button in the Port Status or Port Index box for the COM port you wish to configure; the COM port menu will be displayed. (Remember, the COM port menus are available in all Application Display modes.)
2. Drag down to **UPS**, and release.

If the COM port menu does not include the UPS selection, that COM port has not yet been configured for UPS operation; see **Configuring COM Ports**, page 2-36, for more information.

The UPS configuration tool is described in detail in Chapter 8 of the ***SPMA Tools Guide***.

Accessing FDDI Management

If you have any FDDI modules installed in your 7C0x SmartSwitch chassis, the **Module —> FDDI Utilities** menu provides access to five applications that allow you to monitor and manage your FDDI interfaces.

To access FDDI management applications:

1. Click either mouse button on the Module Index or Module Type box in the Hub View to display the Module menu. (Remember, the Module menu is available in all Application Display modes.)
2. Drag down to **FDDI Utilities**, then across to select the FDDI management tool you need:
   a. **Port Configuration**
   b. **Alarm Configuration**

c. **SMT/MAC Configuration**

d. **SMT Connection Policy**

e. **Station List**

All of these applications are described in detail in Chapter 4, **FDDI Management**.

Accessing ATM Management

For 7C0x SmartSwitches which have a 7A06-01 NIM installed, the Module menu will provide access to the ATM configuration application.

To launch this application:

1. Click either mouse button on the Module Index or Module Type box in the Hub View to display the Module menu. (Remember, the Module menu is available in all Application Display modes.)
2. Drag down to **ATM**, and release.

The ATM Configuration application is described in detail in Chapter 5, **ATM Configuration**.

Accessing Bridge Management

For 7C0x SmartSwitches which are configured to operate as traditional bridges, you can use the Bridge menu to launch the Bridge View application. To do so:

1. If necessary, put the Hub View into the Bridge Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then across to select **Bridge**).
2. Click either mouse button on the Display Mode box in the Hub View to launch the Bridge menu; drag down to **Bridge Mgmt**, and release.

The Bridge View application is described in detail in Chapter 6, **Using the 7C0x SmartSwitch Bridge View**.

Setting the Polling Intervals

To set the polling intervals used by SPMA and the 7C0x SmartSwitch:

1. Click on Device to display the Device menu.
2. Drag down to **Polling Intervals**, and release.

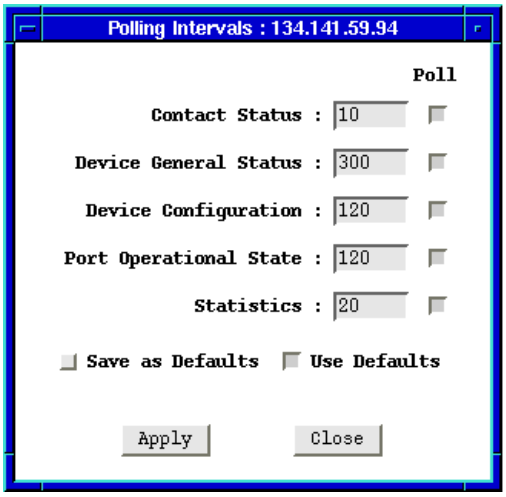


Figure 2-15. 7C0x SmartSwitch Polling Intervals

3. To activate the desired polling, click mouse button 1 on the selection box to the right of each polling type field.
4. To change a polling interval, highlight the value you would like to change, and enter a new value in seconds. Note that the **Use Defaults** option must *not* be selected, or values will revert back to default levels when you click on Apply, and your changes will be ignored.
5. If you wish to use your new polling interval settings as the default values that SPMA will use for each SmartSwitch you are managing, use mouse button 1 to select the **Save As Defaults** option.
6. If you wish to replace existing values with the current set of default values, use mouse button 1 to select the **Use Defaults** option.
7. Click mouse button 1 on Apply once your changes are complete. Changes take effect after the current polling cycle is complete.

You can set the update intervals for the following:

Contact Status
This polling interval controls how often the 7C0x SmartSwitch is "pinged" to check SPMA's ability to maintain a connection with the device.

Device General Status
This polling interval controls how often the Hub View Front Panel Information — such as Uptime, Device Name, and so forth — and some module and port status information is updated.

Device Configuration
This polling interval controls how often a survey is conducted of the type of equipment installed in the 7C0x SmartSwitch hub; information from this poll would change the Hub View to reflect the addition and/or removal of a NIM or NIMs.

Port Operational State
This polling interval controls the update of the information displayed in the Port Status boxes for each port in the hub. Port state information varies according to the Port Display Form which is currently selected.

Statistics
This polling interval controls how often the information displayed in the Port Status boxes is updated when the Port Display Form is set to a rate or percentage.

NOTE

SPMA generates network traffic when it retrieves the above-described information; keep in mind that shorter intervals mean increased network traffic. Range limits for these polling times are 0-999,999 seconds; however, an entry of 0 will be treated as a 1.

Port Configuration

The Port Configuration options available for FDDI, Ethernet, Fast Ethernet, and COM ports allow you to configure operating parameters specific to each port type: for FDDI and standard Ethernet ports, you can set the Duplex Mode; for Fast Ethernet ports, you can set a variety of duplex mode and negotiation parameters; and for COM ports, you can select the operation you wish the port to perform, and set any associated speed parameters. FDDI, Ethernet, and Fast Ethernet Port Configuration windows are available from the Interface Application Display Port menus; the COM Port menu is available in all Application Display modes.

Configuring Ethernet and FDDI Ports

The Port Configuration window available for both Ethernet and FDDI ports allows you to set an interface to either Standard or Full Duplex Mode. Full Duplex mode effectively doubles the available wire speed by allowing the interface to both receive and transmit simultaneously. This window will also display the mode currently in effect on the selected interface.

To access the Port Configuration Window:

1. If necessary, put the Hub View into the Interface Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then across to select **Interface**).

2. Click mouse button 3 on the Port Status box for the Ethernet or FDDI interface whose mode you wish to change.
3. Drag down to **Configuration**, and release**.** The Port Configuration window, Figure 2-16, will appear.

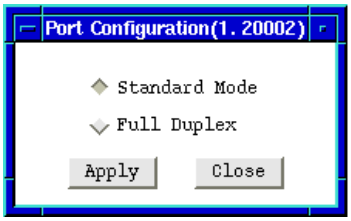


Figure 2-16. Port Configuration

TIP

Note that, if you select the Configuration option available for a Fast Ethernet interface, an entirely different window will appear; see ***Configuring Fast Ethernet Ports****, below, for information on configuring these ports.*

Use the options in this window to select the desired mode:

Standard Mode

In Standard Mode, an interface can only either transmit *or* receive at any given time, and must wait for one activity to be completed before switching to the next activity (receive or transmit). In this mode, standard wire speeds (10 Mbps for Ethernet, 100 Mbps for FDDI) are available.

Full Duplex

In Full Duplex Mode, an interface can both receive *and* transmit packets at the same time, effectively doubling the available wire speed to 20 Mbps (for Ethernet) or 200 Mbps (for FDDI).

Be sure to click on Apply to set your changes.

Note that the interface's current mode can be determined by the field selected in the window; you can also use the Duplex Mode port display form to display the current mode for all installed interfaces. See **Interface Port Display Forms**, page 2-16, for details.

Configuring Fast Ethernet Ports

If you have any Fast Ethernet NIMs installed in your 7C0x SmartSwitch chassis, the Port Configuration window available for those ports allows you to both view and set that port's available modes. All 100Base-TX Fast Ethernet ports can be configured to operate in either standard Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) mode, and in each mode can be configured to operate in Full Duplex, effectively doubling the available wire speed (from 10 to 20 Mbps in standard Ethernet mode, or from 100 to 200 Mbps in Fast Ethernet mode); 100Base-FX (fiber) ports can be configured to operate in their standard 100 Mbps mode, or in full duplex mode. This window also displays the mode currently in effect on the selected interface, and provides some information (where it is available) about the interface's link partner.

To access the Port Configuration Window:

1. If necessary, put the Hub View into the Interface Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then across to select **Interface**).
2. Click mouse button 3 on the Port Status box for the Fast Ethernet interface whose mode you wish to change.
3. Drag down to **Configuration**, and release**.** The Fast Ethernet Port Configuration window, Figure 2-17, will appear.

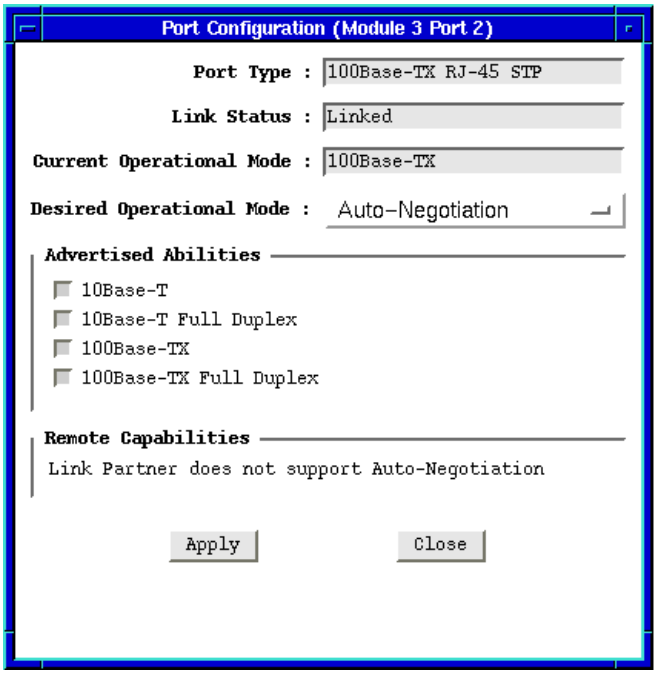


Figure 2-17. Fast Ethernet Configuration

NOTE

The Advertised Abilities functionality is not supported by the FE-100FX Fast Ethernet port module; if you launch the Configuration window for one of these modules, the ***Advertised Abilities*** *section of the window will display No Support, and the* ***Remote Capabilities*** *section will display Unknown. If you launch the window for a port module slot which has no FE module installed, all fields will display either Unknown or No Support.*

TIP

Note that, if you select the Configuration option available for a standard Ethernet or FDDI interface, an entirely different window will appear; see ***Configuring Ethernet and FDDI Ports****, page 2-30, for information on configuring these ports.*

From this window you can manually set the operational mode of the port, or — for 100Base-TX interfaces — set the port to auto negotiation so that the appropriate operational mode can be determined automatically. The mode you set will determine the speed of the port and whether it uses Full Duplex or Standard Mode bridging.

The following information about the selected Fast Ethernet port is displayed:

Port Type

Displays the port's type: 100Base-TX RJ-45 (for built-in Fast Ethernet ports and the FE-100TX Fast Ethernet port module), 100Base-FX MMF SC Connector (for the FE-100-FX Fast Ethernet port module), or Unknown (for a port slot with no module installed).

Link State

Displays the current connection status of the selected port: Linked or Not Linked.

Current Operational Mode

Indicates which of the available operational modes is currently in effect: 10Base-T, 10Base-T Full Duplex, 100Base-TX, 100Base-TX Full Duplex, 100Base-FX, or 100Base-FX Full Duplex. If the port is still initializing, not linked, or if there is no port module installed in the slot, this field will display Unknown.

Desired Operational Mode

Displays the operational mode that you have selected for this port, and allows you to change that selection. The following operational modes are available for each port:

100Base-TX Auto Negotiation, 10Base-T, 10BASE-T Full Duplex, 100Base-TX, and 100Base-TX Full Duplex.

100Base-FX 100Base-FX and 100Base-FX Full Duplex

If you choose to select a specific mode of operation (rather than auto-negotiation), you should be sure that the link partner supports the same mode. Otherwise, no link will be achieved.

If you select a Full Duplex mode and the link partner supports the same wire speed but not Full Duplex, a link will be achieved, but it will be unstable and will behave erratically.

If you select Auto-Negotiation, the local node will try to match the mode of the link partner, even if the link partner is not set to auto-negotiate, and even if the local node must use a mode which is it is not currently advertising.

Note that if Auto Negotiation is the selected mode, the **Current Operational Mode** field will indicate which mode was selected by the link partners.

See **Setting the Desired Operational Mode**, page 2-35, for more information.

Advertised Abilities

For 100Base-TX ports which have been configured to operate in Auto Negotiation mode, this field allows you to select which of the operational modes available to the port can be selected by the negotiating link partners. During Auto Negotiation, each of the link partners will advertise all selected modes in descending bandwidth order: 100Base-TX Full Duplex, 100Base-TX, 10Base-T Full Duplex, and 10Base-T. Of the selected abilities, the highest mode mutually available will automatically be used. If there is no mode mutually advertised, no link will be achieved.

If you have selected a specific operational mode for your 100Base-TX port, the Advertised Abilities do not apply; the selected Advertised Abilities also do not restrict the local node's ability to set up a link with a partner who is not currently Auto-Negotiating.

Auto-Negotiation is not currently supported for 100Base-FX ports; for these ports, the Advertised Abilities section will display ***No Support.***

Remote Capabilities

When the local node is set to Auto-Negotiation, this field will display the advertised abilities of the remote link — even if the remote link is not currently set to auto-negotiate. Possible values for this field are:

- 100Base-TX Full Duplex
- 100Base-TX
- 10Base-T Full Duplex
- 10Base-T

- Link Partner does not support auto negotiation — auto negotiation is either not supported by or is not currently selected on the remote port.
- Unknown — the link partner's capabilities could not be determined.

When the local node is ***not*** set to Auto-Negotiation, this field will remain blank, even if the link partner is set to Auto-Negotiation and is advertising abilities.

NOTE

If both link partners are set to Auto-Negotiation, but there is no mutually-advertised operational mode, no link will be achieved, and both nodes may display the message "Link Partner does not support Auto-Negotiation." To resolve this situation, be sure both link partners advertise all their abilities, or be sure they advertise at least one mutually-available mode.

Setting the Desired Operational Mode

For any 100Base-TX port, you can specifically choose any one of the four available operational modes, or you can select Auto-Negotiation mode, which allows the port to negotiate with its link partner to find the highest mutually available bandwidth. If you select Auto Negotiation mode, you must also choose which of the port's bandwidth capabilities you wish to advertise to the link partner.

TIP

If you select Auto-Negotiation at both ends of a link, be sure at least one mutually-advertised operational mode is available.

For a 100Base-FX port, the selection process is somewhat simpler; Auto Negotiation for these ports is not supported at this time, so you need only choose between 100Base-FX standard mode and 100Base-FX Full Duplex. However, you must still be sure that both link partners are set to the same operational mode, or the link will be unstable.

To set your desired operational mode:

1. Click in the **Desired Operational Mode** field to display the menu of available options; drag down to select the operational mode you wish to set.

   For 100Base-TX ports, the available options are:

   10Base-T — 10 Mbps connection, Standard Mode

   10Base-T Full Duplex — 10 Mbps connection, Duplex Mode

   100Base-TX — 100 Mbps connection, Standard Mode

   100Base-TX Full Duplex — 100 Mbps connection, Duplex Mode

   Auto Negotiation — the operational mode will be dynamically set based on the modes selected in the Advertised Abilities field (where both link partners are auto-negotiating) and the speeds and modes supported by the attached device

For 100Base-FX ports, options are:

100Base-FX — 100 Mbps connection, Standard Mode

100Base-FX Full Duplex — 100 Mbps connection, Duplex Mode

2. If you have selected Auto Negotiation (for 100Base-TX ports only), use the **Advertised Abilities** field to select the operational capabilities you wish to advertise to the port's link partner. If both link partners will be auto-negotiating, be sure there is at least one mutually-advertised operational mode, or no link will be achieved.

TIP

The selected Advertised Abilities only come into play when both link partners are auto-negotiating; if only one link partner is set to auto-negotiate, that node will establish a link at whatever mode its partner is set to, even if that mode is not currently being advertised.

3. Click on Apply to save your changes. Some window fields will refresh immediately and display the new settings; to manually refresh the window, simply close, the re-open it, or just re-select the **Configuration** option from the appropriate Port menu. Note that it may take a few minutes for mode changes to be completely initialized, particularly if the link partners must negotiate or re-negotiate the mode; you may need to refresh the window a few times before current operational data is displayed.

Configuring COM Ports

You can use the COM Port Configuration window (Figure 2-18) to specify the function each of the two RS232 COM ports available on the 7X00 Controller module will perform. To do so:

1. Click mouse button 3 on the Port Status or Port Index box for the COM port you wish to configure. The COM Port Menu will appear; remember, this menu is available in all Application Display modes.

2. Drag down to **Configuration**, and release. The COM Port Configuration window, Figure 2-18, will appear.

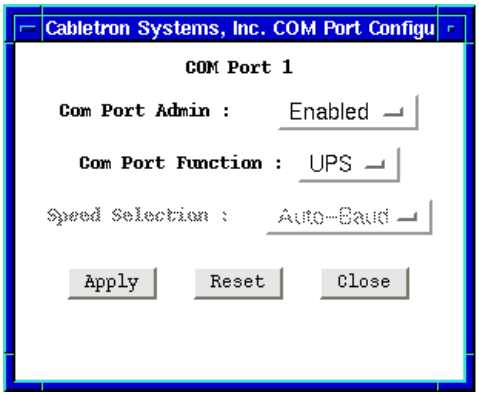


Figure 2-18. COM Port Configuration Window

You can use the COM Port Configuration window to set the following operating parameters:

COM Port Admin

Use this field to administratively enable or disable the COM port.

COM Port Function

Use this field to select the function for which you wish to use the COM port:

LM	Local Management: select this option if you wish to connect a terminal to the selected COM port from which to run Local Management.
UPS	Select this option if you wish to connect an uninterruptable power supply (UPS) to the selected COM Port. Note that if you select this option, an additional option — UPS — will appear on the COM Port menu; use the resulting window to configure specific UPS settings.
SLIP	Select this option to use the selected COM port as a SLIP connection for out-of-band SNMP management via direct connection to a serial port on your network management workstation. Note that when you configure the port as a SLIP connection, you must select the desired baud rate in the **Speed Selection** field described below.
PPP	Select this option to use the selected COM port as a PPP connection for out-of-band SNMP management via direct connection to a serial port on your network management workstation. Note that when you configure the port as a PPP connection, you must select the desired baud rate in the **Speed Selection** field described below.

NOTE

Current 7C0x firmware versions support only Local Management and UPS via the COM port; future versions will add SLIP and PPP support.

Speed Selection

If you have configured the selected port as a SLIP or PPP connection, you must select the appropriate baud rate: 2400, 4800, 9600, 19,200, or Auto-Baud. Note that this field will default to Auto-Baud and become unselectable when the COM Port Function is set to LM or UPS.

TIP

If the COM port you wish to configure is currently set to LM or UPS, the Speed Selection field will be unavailable until the COM Port Function is set to SLIP or PPP and that change is applied. Once available, the Speed Selection field will default to the last known speed setting; click on the field to change this setting if necessary, then click Apply *again to complete the configuration.*

To change any of the configuration parameters on the selected COM port:

1. Click on the **COM Port Admin:** or **COM Port Function:** selection button to display a menu of available options.
2. Drag down to select the desired setting, then release.
3. Click on Apply to save your changes.

Enabling and Disabling Bridge Ports

For devices configured to operate as traditional bridges, you can use the Bridge Port menu (available in the Bridge Application Display mode) or simply click on any Bridge Port index or display box to enable or disable any bridging interface.

To do so:

1. If necessary, put the Hub View into the Bridge Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then across to select **Bridge**).
2. Click mouse button 1 on the bridge interface you wish to enable or disable;

   or

   Click mouse button 3 on the bridge interface you wish to enable or disable to display the Bridge Port menu; drag down to **Enable** or **Disable**, as desired, and release.

3. A window will appear asking you to confirm your selection; click on **OK** to continue the enable or disable process, or on **Cancel** to cancel.

When you disable bridging at a port interface, you disconnect that port's network segment from the bridge entirely. The port does not forward any packets, nor does it participate in Spanning Tree operations. Nodes connected to that network segment can still communicate with one another, but they can't communicate with other networks connected to the bridge.

When you enable bridging for the interface, the port moves from the Disabled state through the Listening and Learning states to the Forwarding state; bridge port state color codes will change accordingly.

NOTE

For more information about bridging functions and how to determine the current state of each bridge port, see ***Bridge Port Display Forms****, page 2-13, and Chapter 6,* ***Using the 7C0x SmartSwitch Bridge View****.*

Chapter 3

Basic Alarm Configuration

Creating alarms; assigning events and actions; viewing an alarm log

Through the RMON Alarm and Event functionality supported by your 7C0x SmartSwitch, you can configure some basic alarm thresholds for each available bridge port interface; you can also define a response to each alarm condition.

CAUTION

The current version of the Basic Alarm application can only be used on devices which are configured to operate as traditional bridges, as it has some dependencies on bridge-specific table information; if you try to launch the application against a device which is configured for SecureFast switching, the window will paint, but the interface list box will remain blank.

About Basic Alarms

Using the Basic Alarm Configuration application, you can define both rising and falling alarm thresholds for three selected MIB-II objects: ifInOctets, ifInNUcast, and ifInErrors. Because these pre-selected objects are not RMON-specific, you can configure alarms for all available bridge interfaces in your SmartSwitch chassis — including those, like FDDI, for which no specific RMON statistics currently exist.

In addition to configuring separate rising and falling thresholds, you can also configure your device's *response* to an alarm condition: when a threshold is crossed, the SmartSwitch can create a log of alarm events, send a trap notifying your management workstation that an alarm condition has occurred, or both; you can even configure an alarm to enable or disable bridging on the offending port in response to a rising or falling alarm condition.

TIP

Current versions of the Basic Alarm Configuration application do not provide a means for viewing any alarm logs you choose to create; if you wish to use the Log option, you can view the associated log via the MIBTree or any similar SNMP-based tool. See ***Viewing an Alarm Log****, page 3-10, for details.*

Launching the Basic Alarm Application

You can access the Basic Alarm application in one of two ways:

from the Hub View:

1. If necessary, put the Hub View into the Interface Application Display mode (click either mouse button on the Module Index or Module Type box to display the Module menu, drag down to **Application Display**, then right to select **Interface**).
2. Click either mouse button on the Display Mode box to launch the Interface menu; drag down to **Basic Alarm Configuration**, and release.

from the command line (stand-alone mode):

1. From the appropriate directory type:

```
spmarun balarm <IP Address> <read community name>
<write community name>
```

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from within the Hub View.*

*If you wish to configure alarms via the Basic Alarm Configuration window, be sure to use a write **community name** with at least Read/Write access. If you only wish to view alarms, a community name with Read access will be sufficient.*

*If there is a hostname mapped to your 7C0x's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is not the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

TIP

If you launch the Basic Alarm application (whether from the Interface menu in the Hub View or from the command line) against a 7C0x whose RMON MIB component has been disabled, an error window will appear notifying you of that fact.

*In many cases the RMON component is disabled by default when the device is shipped; to enable it, use the MIBTree or any similar SNMP-based MIB tool to query the **contLogicalEntryTable**, and change the **contLogicalEntryAdminStatus** value for the RMON component from 7 (disabled) to 3 (enabled). The application should then run successfully.*

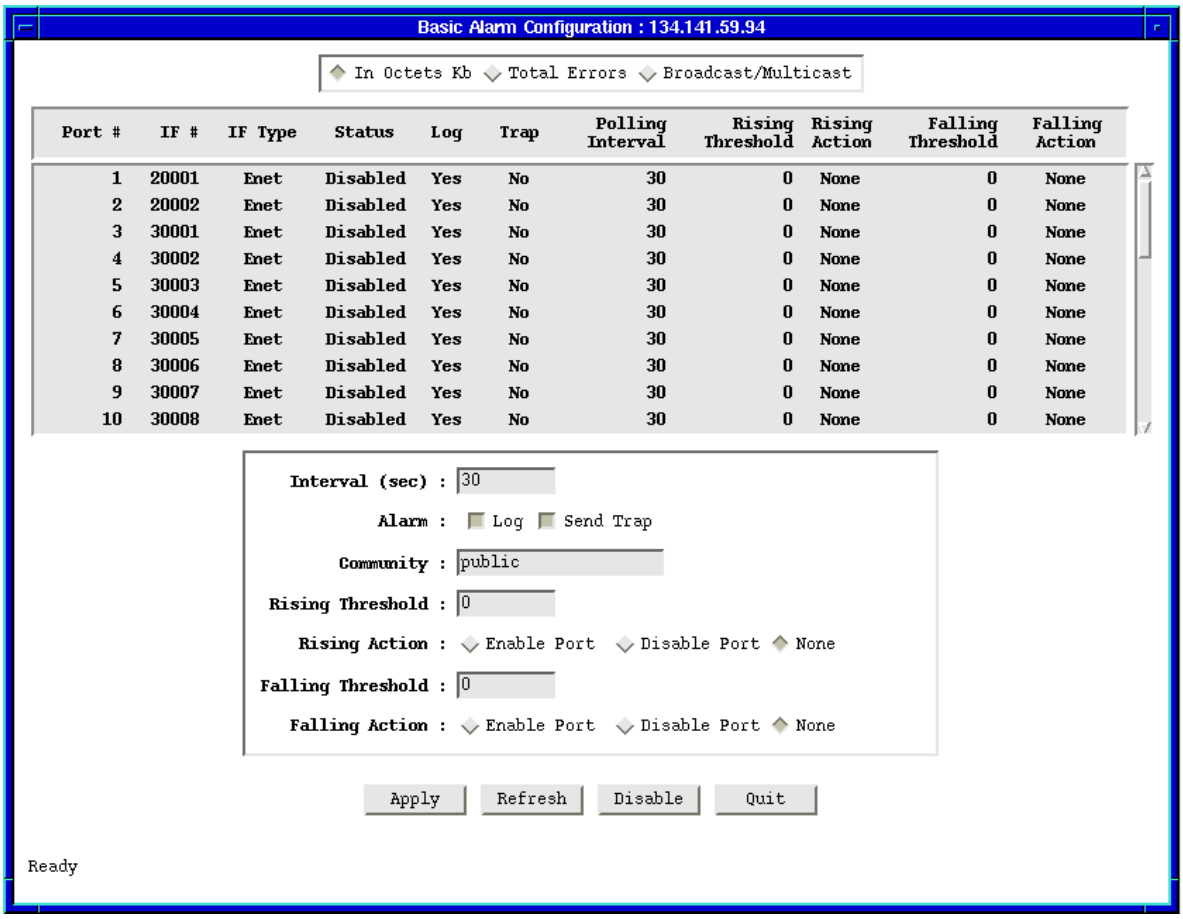


Figure 3-1. Basic Alarm Configuration

Viewing Alarm Status

The Basic Alarm Configuration window, Figure 3-1, contains all the fields you need to configure one or more of the three alarms available for each interface installed in your 7C0x SmartSwitch hub:

In Octets Kb — Total Errors — Broadcast/Multicast

Use these fields at the top of the window to change the alarm type whose status is displayed in the list box. For example, if the **In Octets Kb** option is selected, the information in the list box pertains to the status of the In Octets Kb alarm type for each installed interface. Before you configure an alarm or alarms, be sure the appropriate option is selected here.

The available alarm variables are:

- **In Octets Kb** *(ifInOctets)* — tracks the number of octets of data received by the selected interface. Note that this value has been converted for you from octets (or bytes) to kilobytes (or units of 1000 bytes); be sure to enter your thresholds accordingly. For example, to set a rising threshold of 5000 octets, enter a threshold value of 5; to set a falling threshold of 1000 octets, enter a threshold value of 1.
- **Total Errors** *(ifInErrors)* — tracks the number of error packets received by the selected interface.
- **Broadcast/Multicast** *(ifInNUcast)* — tracks the number of non-unicast — that is, broadcast or multicast — packets received by the selected interface.

TIP

Note that the three pre-selected alarm variables are all MIB II variables; this allows you to configure alarms for any interface installed in your 7C0x SmartSwitch chassis — even those for which no specific RMON statistics yet exist.

Port Number

Provides a sequential indexing of the interfaces installed in your 7C0x SmartSwitch chassis. Available interfaces are indexed from left to right in the hub, and follow physical port indexing on each individual module. (Note that some Ethernet modules index ports from bottom to top, rather than top to bottom; the Port # displayed here will reflect that indexing scheme.)

IF Number

Displays the interface number assigned to each available interface. Interface indexing follows an XXXXYY scheme, where X = slot index times 10,000, and Y = port index. For example, an interface index of 30017 would be assigned to port 17 on the module installed in slot 3 of the chassis.

IF Type

Displays each interface's type: FDDI, Ethernet, or ATM. Note that there is no type distinction between standard Ethernet and Fast Ethernet.

Status

Displays the current status of the selected alarm type for each interface: Enabled or Disabled. Remember, this status refers only to the alarm type which is selected at the top of the window; each of the other two alarm types can have different states.

Log

Indicates whether or not each alarm has been configured to create a silent log of event occurrences and the alarms that triggered them: Yes if it has, No if it hasn't.

TIP

Current versions of the Basic Alarm Configuration application do not provide a means for viewing any alarm logs you choose to create; if you wish to use the Log option, you can view the associated log via the MIBTree or any similar SNMP-based tool. See ***Viewing an Alarm Log****, page 3-10, for details.*

Trap

Indicates whether or not each alarm has been configured to issue a trap in response to a rising or falling alarm condition: Yes if it has, No if it hasn't. Remember, if you choose to select this option for your alarms, you must be sure the 7C0x has been configured to send traps to your management workstation, and that the management workstation you choose has the ability to accept those trap messages. See the **Trap Table** chapter in the ***SPMA Tools Guide*** for more information.

Polling Interval

Displays the amount of time, in seconds, over which the selected alarm variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds (described below). You can set any interval from 1 to 999,999,999 seconds; however, intervals shorter than 10 seconds are not likely to perform well. The default value is 30 seconds.

Rising Threshold

Displays the high threshold value set for the selected alarm variable. By default, values used to compare to the thresholds are relative, or **delta** values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Rising Action

Indicates whether or not a rising alarm occurrence will initiate any actions in response to the alarm condition: Enable if bridging will be enabled at the selected interface in response to a rising alarm, Disable if bridging will be disabled at the selected interface in response to a rising alarm, and None if no actions have been configured for the selected alarm.

Falling Threshold

Displays the low threshold value set for the selected alarm variable. By default, values used to compare to the thresholds are relative, or **delta** values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Falling Action

Indicates whether or not a falling alarm occurrence will initiate any actions in response to the alarm condition: Enable if bridging will be enabled at the selected interface in response to a falling alarm, Disable if bridging will be disabled in response to a falling alarm, and None if no actions have been configured for the selected alarm.

TIP

Before you decided whether or not to assign an action to a rising or falling alarm, it is important to understand something about the hysteresis function built in to the RMON alarm functionality. See ***How Rising and Falling Thresholds Work****, below, for more information.*

The remainder of the window fields provide the means for configuring alarms for each available interface. Note that the information provided in this screen is static once it is displayed; for updated information, click on Refresh. Adding or modifying an alarm automatically updates the list.

How Rising and Falling Thresholds Work

Rising and falling thresholds are intended to be used in pairs, and can be used to provide notification of spikes or drops in a monitored value — either of which can indicate a network problem. To make the best use of this powerful feature, pairs of thresholds should not be set too far apart, or the alarm notification process may be defeated: a built-in hysteresis function designed to limit the generation of events specifies that, once a configured threshold is met or crossed in one direction, no additional events will be generated until the opposite threshold is met or crossed. Therefore, if your threshold pair spans a wide range of values, and network performance is unstable around either threshold, you will only receive one event in response to what may be several dramatic changes in value. To monitor both ends of a wide range of values, set up two pairs of thresholds: one set at the top end of the range, and one at the bottom. Figure 3-2 illustrates such a configuration.

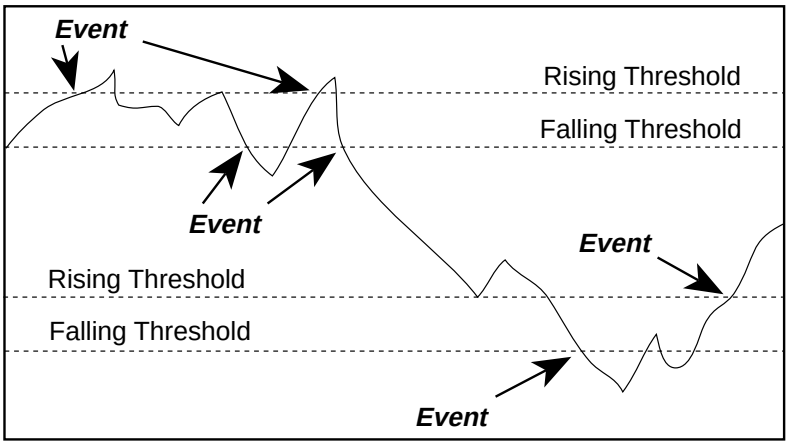


Figure 3-2. Sample Rising and Falling Threshold Pairs

TIP

The current version of the Basic Alarm application only allows you to configure a single pair of thresholds for each alarm variable on each interface; be sure to keep this hysteresis function in mind when configuring those threshold values.

Configuring an Alarm

The editable fields at the bottom of the Basic Alarm Configuration window allow you to configure alarm parameters for each available interface. These fields will display the alarm parameters for the interface which is currently highlighted (and the alarm variable currently selected at the top of the window); if more than one interface is selected in the list box, the parameters displayed will be those assigned to the selected interface with the lowest index number.

Note that there is no specific "Enable" function; simply configuring thresholds and/or actions for an alarm and applying those changes enables the alarm. For more information on disabling an alarm, see **Disabling an Alarm**, page 3-9.

To configure an alarm:

1. At the top of the window, click to select the variable to be used for your alarm: **In Octets Kb**, **Total Errors**, or **Broadcast/Multicast**. The display in the list box will reflect the current status at each interface of the alarm type you have selected.
2. In the list box, click to highlight the interface or interfaces for which you would like to configure an alarm for the selected variable. Note that the editable fields will display the alarm parameters assigned to the selected interface with the lowest index number; however, any changes you make in these fields will be set to *all* selected interfaces.
3. In the **Interval** field, enter the amount of time, in seconds, over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. You can assign any interval from 1 to 999,999,999; however, intervals shorter than 10 seconds are not likely to perform well. The default value is 30.
4. In the **Alarm** field, click to select one or both of the following options:
   a. Select **Log** if you wish to create a silent log of alarm occurrences.
   b. Select **Trap** if you wish the 7C0x to issue a trap in response to each alarm occurrence.

NOTES

Current versions of the Basic Alarm Configuration application do not provide a means for viewing any alarm logs you choose to create; if you wish to use the ***Log*** *option, you can view the associated log via the MIBTree or any similar SNMP-based tool. See* ***Viewing an Alarm Log****, page 3-10, for details.*

If you select the ***Trap*** *option, be sure your 7C0x SmartSwitch is configured to send traps to your management workstation, and be sure that workstation has the ability to receive traps (which SPMA does not provide); for more information, see the* ***Trap Table*** *chapter in the* **SPMA Tools Guide**.

5. If you have selected the Trap option in the Alarm field, the **Community** field will become active; any value you enter here will be included in any trap messages. Your trap utility may use this community name as a means of filtering traps, or as a means of directing traps within the management platform; if it does not, you need not enter a value into this field. A value of "public" will be assigned by default.

6. Click in the **Rising Threshold** field; enter the high threshold value for this alarm. Remember, compared values are always relative, or delta values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

   Remember, too, when configuring an **In Octets Kb** alarm, SPMA converts octets into kilobytes for you; for example, to set a rising threshold of 5000 octets, enter a threshold value of 5.

7. In the **Rising Action** field, click to select the action you want your device to take in response to a rising alarm: Enable Port, Disable Port, or None. Note that this action enables and disables only *bridging* at the specified port, and not the interface itself.

   For more information on how actions are triggered, see **How Rising and Falling Thresholds Work**, page 3-6.

8. Click in the **Falling Threshold** field; enter the low threshold value for this alarm. Remember, compared values are always relative, or delta values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

   Remember, too, when configuring an **In Octets Kb** alarm, SPMA converts octets into kilobytes for you; for example, to set a falling threshold of 2000 octets, enter a threshold value of 2.

9. In the **Falling Action** field, click to select the action you want your device to take in response to a falling alarm: Enable Port, Disable Port, or None. Note that this action enables and disables only *bridging* at the specified port, and not the interface itself.

   For more information on how actions are triggered, see **How Rising and Falling Thresholds Work**, page 3-6.

10. Click [Apply] to set your changes. If you have made any errors in configuring alarm parameters (using an invalid rising or falling thresholds, for example), an error window with the appropriate message will appear. Correct the noted problem(s), and click [Apply] again.

Once you click [Apply], the configured alarm parameters will be set for every selected interface, and the alarms will automatically be enabled; the list box display will also refresh to reflect these changes.

To configure additional alarms, or alarms of a different type, select the appropriate alarm variable at the top of the window, highlight the appropriate interface(s), and repeat the procedures outlined above.

Disabling an Alarm

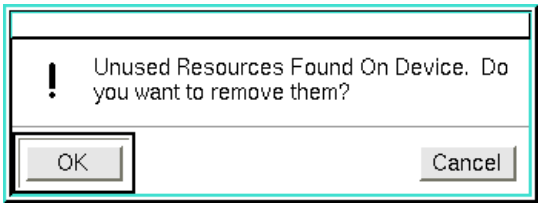
Using the Disable button at the bottom of the window actually performs two functions: it both disables the alarm and deletes the alarm entry (and its associated event and action entries) from device memory to help conserve device resources. In the list box display, any "disabled" alarm automatically resets to the default parameters: status disabled, log yes, trap no, rising and falling thresholds zero, and no action.

To disable an alarm:

1. In the top of the window, click to select the variable for which you wish to disable an alarm: **In Octets Kb**, **Total Errors**, or **Broadcast/Multicast**.
2. In the list box display, click to highlight the interface(s) for which you wish to disable the selected alarm type. Remember, the editable fields in the lower portion of the window will display the alarm parameters for the selected interface with the lowest index number, but the selected alarm type will be disabled for all selected interfaces.
3. Click on Disable. The selected alarm type on the selected interface(s) will be disabled, and the list box display will refresh to reflect those changes.

NOTE

When you disable an alarm, the SPMA Basic Alarm Configuration application deletes the alarm entry and its associated event (log and/or trap) and action (enable or disable port) entries from device memory. However, if any one of these delete operations fails, some unused entries may remain in the tables. If this occurs, you will see the following error message the next time you launch the Basic Alarm application or click the ***Refresh*** *button:*



To delete these unused entries and free up all available device resources, click ***OK****; to leave the entries there, click* ***Cancel****. Note that this message will re-appear each time you launch the application or click the* ***Refresh*** *button until the unused entries have been removed.*

Viewing an Alarm Log

The ability to create a log of alarm events is provided by the Event group of the RMON MIB. If you have selected the Log option for any of your alarms, and you wish to view the resulting log, you can do so by using MIBTree or any similar SNMP-based MIB tool to query the RMON MIB's **logTable**.

CAUTION

Making sense of a logTable entry by viewing its values straight from the MIB is a tricky business that requires a good understanding of MIBs and MIB objects, a good understanding of the RMON alarm and event functionality, and a little bit of luck: individual returned MIB values must first be sorted into complete entries; each entry must then be matched to the appropriate interface. This process will require some patience, especially if you are viewing the logTable for a 7C0x chassis with many installed interfaces, many of which have enabled alarms. Future releases of SPMA will include more advanced alarm functionality, including the ability to view alarm logs in an easy-to-read format.

Each entry in the logTable (logEntry) contains the following objects:

logEventIndex

The value of this object reflects the index number assigned to the event whose occurrences you have chosen to log. (The "event" is the device's response to the "alarm" — if an *alarm* threshold is crossed, the *event* specifies what action will be taken. The Basic Alarm application allows you to create three kinds of events: those that create a log, those that generate a trap, and those that do both.) The value of this index number won't tell you which interface the alarm instances occurred on; however, it will help you to figure out which values of the logIndex, logTime, and logDescription OIDs go together, as this value becomes part of the instance assigned to each object in the table.

logIndex

The value of this object uniquely identifies each alarm occurrence that is stored in a log entry. In combination with the logEventIndex value described above, the logIndex provides the instance values assigned to each table object; use these instance values to sort out individual log entries. For example, the values of all logTable OIDs with the instance 7.1 apply to the first occurrence of alarm index 7; the values of all OIDs with the instance 7.2 apply to the second occurrence of alarm index 7; and so on.

TIP

Use the instance values assigned to each table object (logEventIndex.logIndex) to arrange the returned values into complete entries; then, view each entry's logDescription to match the entry to a 7C0x interface. See ***logDescription****, below, for more information.*

logTime

Displays the value of the 7C0x's sysUpTime when the alarm instance occurred (in timeticks by default, but perhaps converted by your MIB utility into days hours:minutes:seconds format). You can compare this value to the device's current *sysUpTime* to get a general idea when the alarm condition occurred.

logDescription

The logDescription object provides a detailed description of the alarm event, including a piece of information critical to making sense of the logTable information: the OID of the alarm variable, including its *instance* — which corresponds to the 7C0x *interface* on which the alarm was configured. (The instance value is the last value in the OID string.) Other descriptive information provided includes whether it was a rising or falling event, the index number assigned to the alarm, the alarmSampleType (always 2, or delta), the value that triggered the alarm, the configured threshold that was crossed, and a description of the alarm occurrence (either Falling Threshold or Rising Threshold).

Note that each logTable will hold only a finite number of entries, which is determined by the resources available on the device; when the log is full, the oldest entries will be replaced by new ones.

Chapter 4

FDDI Management

Using the FDDI utilities to manage FDDI modules: port configuration, alarm configuration, SMT/MAC configuration, configuring the connection policy, and viewing the station list

The Module menu FDDI Utilities selections allow you to monitor and manage the FDDI interfaces installed in your 7C0x SmartSwitch hub. Each of the applications available via this menu is described in this chapter:

- **Port Configuration** lets you view information about the state of the FDDI interfaces on your module, and allows you to administratively enable or disable individual A and B ports.
- **Alarm Configuration** allows you to set the LER Alarm and LER Cutoff thresholds for the FDDI interfaces installed in the SmartSwitch hub.
- **SMT/MAC Configuration** lets you see information about the configuration of your FDDI modules' Station Management (SMT) entities, the operating state of the ring to which each is connected, the physical state of the PHY A and B front panel ports, and parameters related to ring initialization.
- **SMT Connection Polic**y lets you determine which types of connections will be permitted among the four FDDI port types: A, B, M (Master), and S (Slave).
- The **Station List** application allows you to view a list of all stations on the FDDI ring to which each FDDI interface is connected, along with some general information about each station.

NOTES

Each of the FDDI applications available for your 7C0x SmartSwitch can be launched either from within the Hub View or from the command line; note, however, that when an application is launched from the command line, it cannot perform the same kind of port mapping the Hub View can provide, so all port indexing will be handled based on SMT index and port physical index, rather than by front panel index (FP 1 or FP 2) and port type (A or B). All other functionality is identical.

Note, too, that due to a software anomaly, port mapping is not provided for any hub which contains more than one FDDI module; that is, ports will be indexed by SMT and port physical index, rather than by front panel index and port type. Future versions of SPMA will correct this anomaly.

Port Configuration

The Port Configuration window (Figure 4-1) displays information about the configuration of the ports on your FDDI modules, and allows you to enable or disable those ports.

To open the Port Configuration window

from the Hub View:

1. Click either mouse button on any Module Index or Module Type text box to display the Module Menu (remember, this menu is the same for all application display modes).
2. Drag down to **FDDI Utilities**, then across to select **Port Configuration**.

from the command line (stand-alone mode):

1. From the appropriate directory type:

```
spmarun fddiptcf <IP Address> <community name>
```

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from within the Hub View.*

*If you wish to enable or disable any ports via the Port Configuration window, be sure to use a **community name** with at least Read/Write access. If you only wish to view port configuration, a community name with Read access will be sufficient.*

*If there is a hostname mapped to your 7C0x's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is not the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

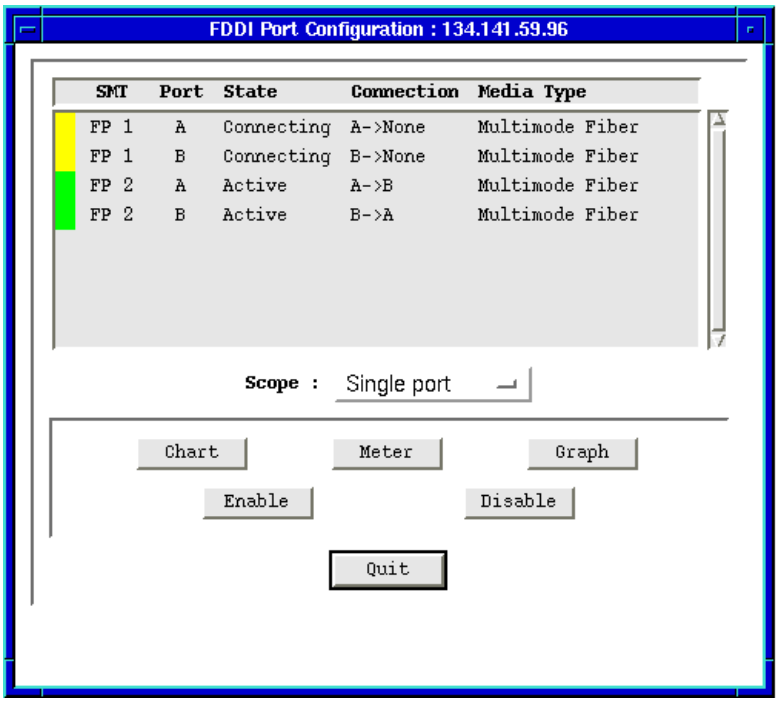


Figure 4-1. Port Configuration Window

The Port Configuration window displays the following information:

SMT Index

Displays the index number of the Station Management (SMT) entity to which each port is attached. Each FDDI NIM module has two SMT entities — one for each front panel interface. If you have launched the Port Configuration application from the Hub View Module menu, these two SMT entities will be indexed by front panel interface numbers (FP 1 and FP 2, as illustrated above); if you have launched the application from the command line (or if your 7C0x hub has more than one FDDI NIM installed), the front panel designations will not appear. For multiple NIMs, SMT entities will be indexed from left to right in the hub, and from top (front panel port 1) to bottom (front panel port 2) on each module.

Port Index

Displays the index number assigned to each port. If you have launched the Port Configuration application from the Hub View, each front panel port will be identified by type (A or B); if you have launched from the command line, each will be identified by a logical index number (1 or 2) that identifies the port in relation to its assigned SMT entity.

State

Displays a value that indicates the port's connection status. There are four possible connection states:

- **Connecting —** the port is trying to establish a link, but has not yet been successful. Ports which are not connected and which have not been disabled by management will display this status.
- **Active —** the port has been enabled by management and has successfully established a link with its downstream neighbor.
- **Standby —** the port has a physical link, but the SMT Connection Policy is prohibiting a logical connection to the ring because the attempted connection is illegal. FDDI protocol always forbids connecting two Master ports; all other connections are theoretically legal, although some are not desirable.

NOTE

*Refer to **Configuring the SMT Connection Policy**, page 4-21, for more information.*

- **Disabled —** the port has been disabled by management; note that this status does not indicate whether or not there is a physical link connected to the port.

Connection

A port's connection is defined by its own port type (A or B) and the port type to which it is connected. For example, a normal connection for a FDDI A port would be **A—>B** (a "thru" configuration); a port that has no connection will display as **B—>None**.

Media Type

Indicates the type of cable segment connected to the port; possible values are:

- Multimode Fiber
- Single Mode Fiber 1
- Single Mode Fiber 2
- SONET
- Low-cost Fiber
- Twisted Pair
- Unknown (firmware can't locate the information)
- Unspecified (information is not included in the firmware)
- ? (firmware is not responding to the request)

Enabling or Disabling FDDI Ports

You can enable or disable ports individually or as a group, as follows:

1. Highlight the appropriate port or ports in the scroll list. You can select or de-select any ports by clicking on them, or you can use the **Scope** field: if you select *All Ports*, all available ports will be automatically selected; if you select *Single Port*, only the port last selected will remain selected (or all ports will be de-selected, allowing you to select one). Note that the setting displayed in the **Scope** field will automatically adjust as you select and de-select ports.
2. Click on either Enable or Disable. The appropriate window shown in Figure 4-2 will appear.

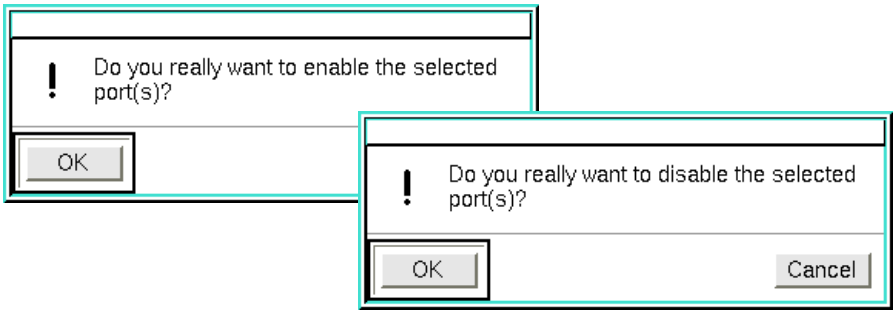


Figure 4-2. Enable/Disable Confirmation Windows

3. Click OK to enable or disable the port, or click Cancel to terminate the command and exit the window.

Charts, Graphs, and Meters

You can view both an FDDI Port Chart and FDDI Port Meters (and, if you are running SPMA in conjunction with HP Network Node Manager or IBM NetView, an FDDI Port Graph) for your module by clicking on the appropriate buttons, located at the bottom of the Port Configuration window.

NOTES

Graphing capabilities are provided by an application that is included in HP Network Node Manager and IBM NetView; therefore, graphs are only available when SPMA is run in conjunction with one of these network management platforms. If you are running SPMA in a stand-alone mode or in conjunction with SunNet Manager, no graphing capabilities are available and no graph-related options will be displayed on buttons or menus. Note that the screens displayed in this guide will include the graph-related options where they are available; please disregard these references if they do not apply.

Only general information about charts, graphs, and meters is provided in the following sections; for more detailed information, see the **SPMA Tools Guide.**

Viewing the FDDI Port Chart

To view the FDDI Port Chart window, highlight an entry in the scroll list and click [Chart]. The FDDI Port Chart window, Figure 4-3, will appear.

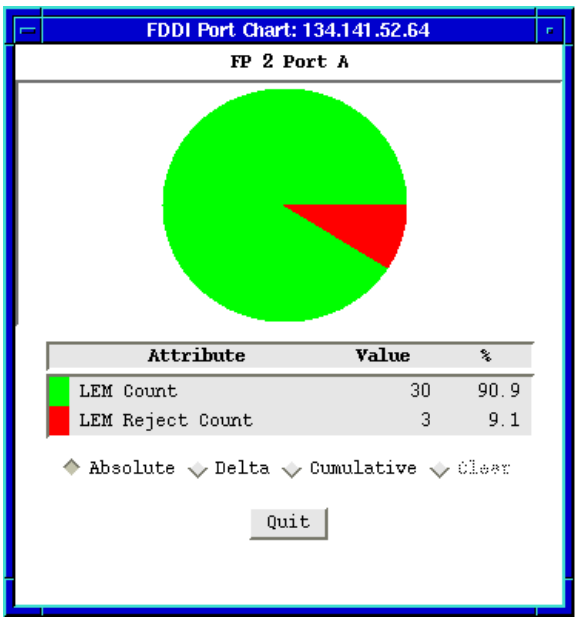


Figure 4-3. FDDI Port Chart Window

The FDDI Port Chart window displays the following information about the selected port or ports, in both numeric and graphical format:

LEM Count

The LEM (Link Error Monitor) Count displays the number of times each port's Link Error Monitor has detected a link error. A link error occurs when a port's line state goes from Idle to Unknown and remains there for at least 80 ns, or when the line state goes from Active to Unknown and remains there for at least 320 ns. A growing LEM Count usually indicates a physical problem with the connectors or the cable between a port and the node at the other end of its cable segment. If you can wiggle the cable and watch the LEM Count increase, you know you have a faulty cable or connector. Dirt or film on the connector cable ends can also add to the LEM Count.

LEM Reject Count

The number of times the port's link has exceeded the configured LER Cutoff level and been removed as faulty (disabled by station management). SMT automatically re-enables a port when the error rate falls below the cutoff value. See **Alarm Configuration**, page 4-9, for more information on setting the LER Cutoff threshold.

Changing the Measurement of Data

Measurement fields located at the bottom of the FDDI Port Chart window allow you to change how the incoming data is measured:

- **Absolute —** displays the chart variable values recorded in the device MIB counters.
- **Delta —** displays the difference in value for the selected data between the current poll interval and the last interval.
- **Cumulative —** displays the total since the Cumulative button was selected.
- **Clear —** resets Cumulative totals to zero; this option is not available in the Absolute or Delta modes.

To change the type of measurement, or to clear and restart Cumulative totals, click mouse button 1 on the appropriate shadowed button.

To exit the FDDI Port Chart window, click [Quit].

Viewing FDDI Port Meters

To view the FDDI Port Meters window, highlight one or more ports in the scroll list and click [Meter]. The FDDI Port Meters window, Figure 4-4, will appear. Each of the meters provided displays a single statistic in a format that lets you know at a glance if the counter is registering high, medium, or low values.

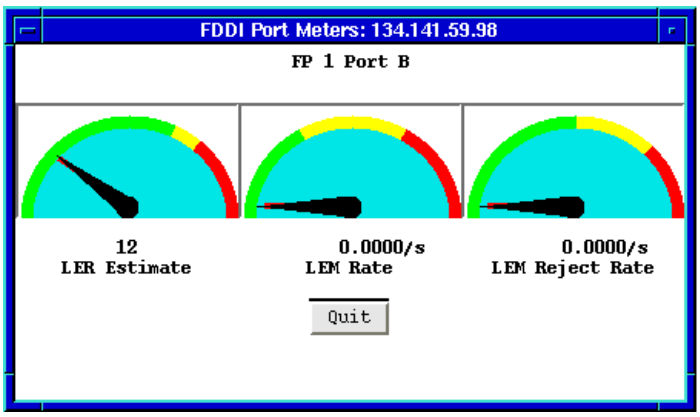


Figure 4-4. FDDI Port Meters Window

The FDDI Port Meters window graphically displays the following statistics:

LER Estimate

The LER (Link Error Rate) Estimate displays a cumulative long term average of the bit error rate, which represents the quality of the physical link. It is computed when the port is connected, and every 10 seconds thereafter. The value of the LER

Estimate can range from 10^{-4} to 10^{-15}, but is always displayed as the absolute value of the exponent; for example, if the port's LER Estimate is computed to be 10^{-5}, the value displayed in the Port Status box will be 5, which represents an actual rate of 1,250 bit errors per second. The lower LER Estimate numbers represent the highest bit error rates.

LEM Rate

The LEM (Link Error Monitor) Rate displays the number of times each port's Link Error Monitor has detected a link error, expressed as link errors per second. A link error occurs when a port's line state goes from Idle to Unknown and remains there for at least 80 ns, or when the line state goes from Active to Unknown and remains there for at least 320 ns. A growing LEM Count usually indicates a physical problem with the connectors or the cable between a port and the node at the other end of its cable segment. If you can wiggle the cable and watch the LEM Count increase, you know you have a faulty cable or connector. Dirt or film on the connector cable ends can also add to the LEM Count.

LEM Reject Rate

The number of times the port's link has exceeded the configured LER Cutoff level and been removed as faulty (disabled by station management), expressed as rejects per second. SMT automatically re-enables a port when the error rate falls below the cutoff value.

To exit the FDDI Port Meters window, click Quit.

NOTE

*See **Alarm Configuration**, page 4-9, for more information on the statistics described above and their associated alarms.*

Viewing FDDI Port Graphs

If you are running SPMA in conjunction with HP Network Node Manager or IBM NetView, the Port Configuration window will include a **Graph** button; select this button to display FDDI variables for the selected port via the graphing application provided by your network management platform.

If you are running SPMA in conjunction with SunNet Manager or in a stand-alone mode, no graphing capabilities are available, and no graph-related options will appear.

Alarm Configuration

The Alarm Configuration application allows you to set the LER Alarm and LER Cutoff thresholds for each FDDI interface installed in the SmartSwitch chassis. Once alarms have been configured, a port will enter an alarm state if its LER Estimate exceeds the LER Alarm threshold; if the LER Estimate exceeds the LER Cutoff threshold, the port will be disabled.

To open the Alarm Configuration window (Figure 4-5):

from the Hub View:

1. Click either mouse button on any Module Index or Module Type text box to display the Module Menu (remember, this menu is the same for all application display modes).
2. Drag down to **FDDI Utilities**, then across to select **Alarm Configuration**.

from the command line (stand-alone mode):

1. From the appropriate directory type:

```
spmarun fddialrm <IP Address> <community name>
```

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from within the Hub View.*

*If you wish to configure any alarm thresholds, be sure to use a **community name** with at least Read/Write access. If you only wish to view alarms, a community name with Read access will be sufficient.*

*If there is a hostname mapped to your 7C0x's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is not the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

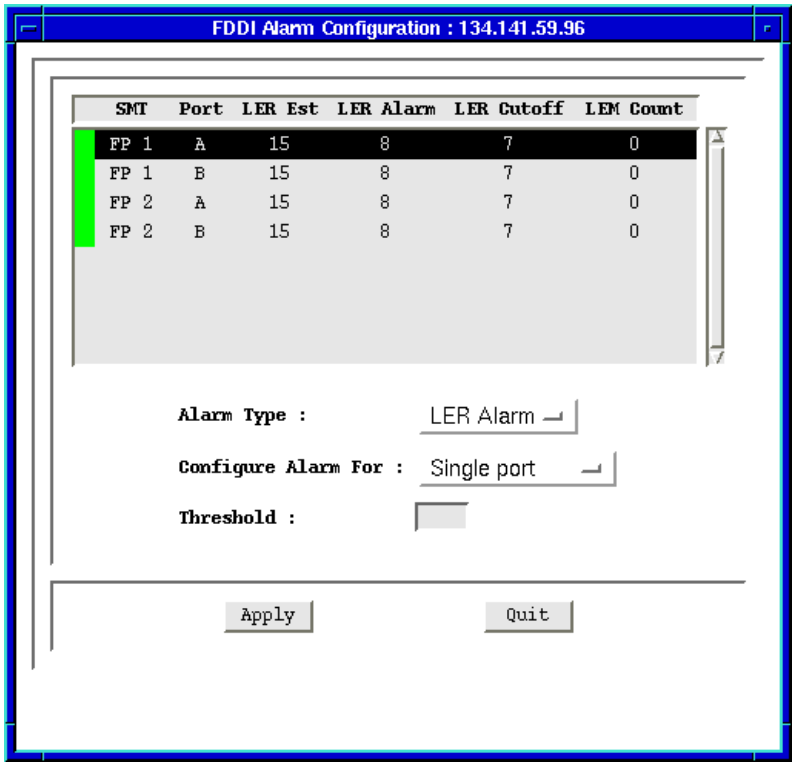


Figure 4-5. Alarm Configuration Window

The Port List Box in the upper portion of the window displays the following information for each FDDI port in the hub:

(Port Alarm Status)

The color displayed in this box indicates the LER Alarm status of each listed port: green indicates that the port's LER Estimate is below the LER Alarm threshold; yellow indicates that the port's LER Estimate has equaled or exceeded the LER Alarm threshold, and the port is in an alarm state; and red indicates that the port's LER Estimate has equaled or exceeded the LER Cutoff threshold, and the port has been disabled.

SMT Index

Displays the index number of the Station Management (SMT) entity to which each port is attached. Each FDDI NIM module has two SMT entities — one for each front panel interface. If you have launched the Alarm Configuration application from the Hub View Module menu, these two SMT entities will be indexed by front panel interface numbers (FP 1 and FP 2, as illustrated above); if you have launched the application from the command line (or if your 7C0x hub has more than one FDDI NIM installed), the front panel designations will not

appear. For multiple NIMs, SMT entities will be indexed from left to right in the hub, and from top (front panel port 1) to bottom (front panel port 2) on each module.

Port

Displays the index number assigned to each port. If you have launched the Alarm Configuration application from the Hub View, each front panel port will be identified by type (A or B); if you have launched from the command line, each will be identified by a logical index number (1 or 2) that identifies the port in relation to its assigned SMT entity.

LER Estimate

The Link Error Rate (LER) Estimate (Figure 4-6) is a cumulative long term average of the bit error rate, which represents the quality of the physical link. It is computed when the port is connected and every 10 seconds thereafter. The value of the LER Estimate can range from 10^{-4} to 10^{-15}, but it is always displayed as the absolute value of the exponent; for example, if the port's LER Estimate is computed to be 10^{-5}, the value displayed will be 5, which represents an actual rate of 1,250 bit errors per second. The lowest LER Estimate numbers represent the highest bit error rates, as summarized in the figure below.

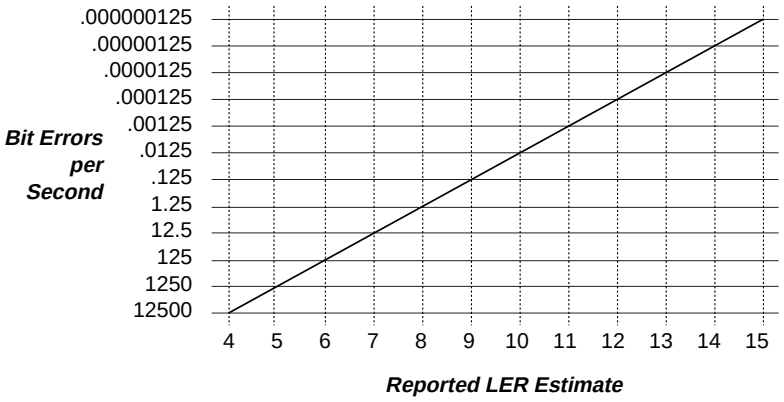


Figure 4-6. LER Estimate Values

LER Alarm

The Link Error Rate (LER) Alarm field displays the threshold at which a port will enter an alarm condition. A port in an alarm condition will display a yellow status in the Alarm Configuration window; in addition, you can configure the Meters application so that a mail message will be generated when the threshold is crossed. (For more information about the Meters application, see the **Charts, Graphs, and Meters** chapter in your ***SPMA Tools Guide***.) The default LER Alarm value is 8, which represents 1.25 bit errors per second (see the table above). When configuring the LER Alarm threshold, be sure that the value you set represents a *lower* link error rate than the LER Cutoff threshold, explained below. Remember, a *lower* link error rate is represented by a *higher* threshold setting.

LER Cutoff

The Link Error Rate (LER) Cutoff field displays the threshold at which a connection is flagged as faulty and the port is disabled by Station Management (SMT). SMT automatically re-enables the port when the error rate falls below the cutoff value. The default LER Cutoff threshold is 7, which represents 12.5 bit errors per second (see the table above). When configuring the LER Cutoff threshold, be sure that the value you set represents a *higher* link error rate than the LER Alarm threshold, explained above. Remember, a *higher* link error rate is represented by a *lower* threshold setting.

LEM Count

The Link Error Monitor (LEM) Count field displays the number of times each port's Link Error Monitor detects a link error. A link error occurs when a port's line state goes from Idle to Unknown and remains there for at least 80 ns, or when the line state goes from Active to Unknown and remains there for at least 320 ns. A growing LEM Count usually indicates a physical problem with the connectors or the cable between a port and the node at the other end of its cable segment. If you can wiggle the cable and watch the LEM Count increase, you know you have a faulty cable or connector. Dirt or film on the connector cable ends can also add to the LEM count.

The lower portion of the window provides the fields you need to configure the alarms:

1. In the **Port List Box**, select the port or ports for which you would like to edit the alarm thresholds. You can select or de-select any ports by clicking on them, or you can use the **Configure Alarm For** field: if you select *All Ports*, all available ports will be automatically selected; if you select *Single Port*, only the port last selected will remain selected (or all ports will be de-selected, allowing you to select one). Note that the setting displayed in the **Set Alarm For** field will automatically adjust as you select and de-select ports.

2. In the **Alarm Type** field, select the alarm variable for which you would like to configure a new threshold: LER Alarm or LER Cutoff.

3. Enter your desired alarm threshold in the **Threshold** field. The default LER Alarm threshold is 8, and the default LER Cutoff threshold is 7; the allowable range for both is 4-15. When re-configuring thresholds, remember that *higher* link error rates are represented by *lower* threshold settings; also, be sure to set the threshold for the LER Alarm so that it represents a *lower* link error rate (i.e., has a *higher* setting) than the LER Cutoff threshold. See above for a complete description of the link error rate and how rates are represented.

4. Click on Apply to save your changes. If you wish to configure both LER Alarm and LER Cutoff thresholds, be sure to click on Apply before switching from one to the other, or the changes you made to the first alarm will be lost.

SMT/MAC Configuration

The SMT (Station Management)/MAC (Media Access Control) Configuration window displays information about the configuration of each SMT entity present in the hub, the operating state of the ring to which that entity is attached, the physical state of the A and B ports on each module with respect to their MAC entity, and parameters relating to ring initialization.

To open the SMT/MAC Configuration window (Figure 4-7):

from the Hub View:

1. Click either mouse button on any Module Index or Module Type text box to display the Module Menu (remember, this menu is the same for all application display modes).
2. Drag down to **FDDI Utilities**, then across to select **SMT/MAC Configuration**.

from the command line (stand-alone mode):

1. From the appropriate directory type:

```
spmarun fddicnfg <IP Address> <community name>
```

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from within the Hub View.*

*A **community name** with Read access is sufficient to view SMT/MAC configuration.*

*If there is a hostname mapped to your 7C0x's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is not the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

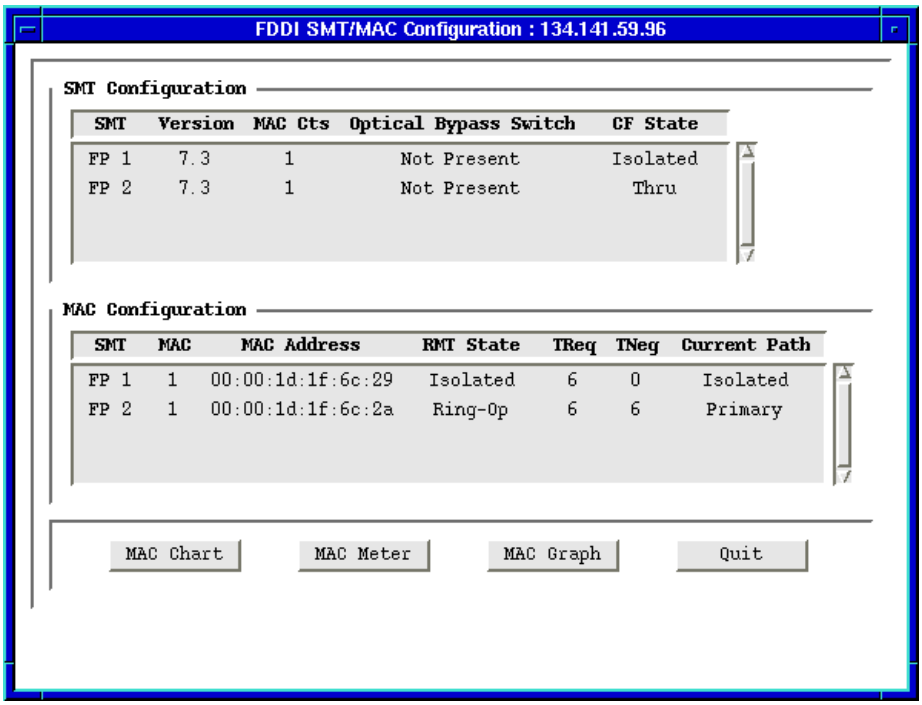


Figure 4-7. SMT/MAC Configuration Window

The SMT Configuration portion of the window provides the following information about the current configuration of each SMT entity present in the SmartSwitch chassis:

SMT Index

Displays the index number of the Station Management (SMT) entity to which each port is attached. Each FDDI NIM module has two SMT entities — one for each front panel interface. If you have launched the SMT/MAC Configuration application from the Hub View Module menu, these two SMT entities will be indexed by front panel interface numbers (FP 1 and FP 2, as illustrated above); if you have launched the application from the command line (or if your 7C0x hub has more than one FDDI NIM installed), the front panel designations will not appear. For multiple NIMs, SMT entities will be indexed from left to right in the hub, and from top (front panel port 1) to bottom (front panel port 2) on each module.

Version

Displays the operational SMT version being used by each SMT entity. SMT frames have a version ID field that identifies the structure of the SMT frame Info field. The version number is included in the SMT frame so that a receiving station can determine whether or not its SMT version is able to communicate with the SMT version of another station. Knowing the version number allows the stations to handle version mismatches. Each FDDI station supports a range of SMT versions.

The supported version range is identified with the ietf-fddi MIB by two smtTable attributes: **fddimibSMTLoVersionId** and **fddimibSMTHiVersionId**. If a received frame is not within the supported version range, the frame is discarded.

MAC Cts

Displays the number of Media Access Control (MAC) entities assigned to each SMT entity.

Optical Bypass Switch

Indicates whether an Optical Bypass Switch is attached to the module's A and B ports. An Optical Bypass Switch can prevent a faulty node from causing a wrap condition or bringing down the ring by bypassing the faulty station and allowing the signal to continue to the next station in the ring.

CF State

The CF (Configuration Management) State displays a value that represents the paths — or ring segments — in which the A and B ports are currently inserted; possible values are:

- **Isolated —** the node is isolated from all available rings.
- **Local-A —** the A port is inserted into a local path; the B port is not inserted into a local path.
- **Local-B —** The B port is inserted into a local path; the A port is not inserted into a local path.
- **Local-AB —** both the A and B ports are inserted into a local path.
- **Wrap-A —** the secondary path is wrapped to the A port.
- **Wrap-B —** the secondary path is wrapped to the B port.
- **Wrap-AB —** the primary path is wrapped to the B port, and the secondary path is wrapped to the A port.
- **C-Wrap-A —** the primary and secondary paths are joined internal to the node, and wrapped to the A port.
- **C-Wrap-B —** the primary and secondary paths are joined internal to the node, and wrapped to the B port.
- **C-Wrap-AB** — The primary path is wrapped to the B port and the secondary path is wrapped to the A port.
- **Thru —** the primary path enters the A port, and exits from the B port; the secondary path enters the B port, and exits from the A port.
- **? —** SPMA cannot determine the current CF State.

The MAC Configuration portion of the window provides the following information about the current configuration of the selected interface's MAC entity:

SMT
Displays the index number assigned to the SMT entity.

MAC
The index number assigned to each MAC entity currently associated with the noted SMT entity. Currently, no more than one MAC can be assigned to each SMT, so this field will always display a 1.

MAC Address
Displays the factory-set hardware address of each available MAC interface.

RMT State
Indicates the current state of the noted MAC's Ring ManagemenT (RMT) state machine. The RMT state machine reports the MAC's current state, which includes Beacon conditions, Trace conditions, and normal conditions.

- **Isolated —** the MAC is not operational because it is not associated with any physical path. This state is also the first state the MAC enters on power-up.
- **Non-Op —** the MAC being managed is participating in ring recovery, and the ring is not operational. The RMT state machine transitions into this state on the loss of Ring_Operational status, and leaves this state on assertion of Ring_Operational.
- **Ring-Op —** the MAC being managed is part of an operational FDDI ring.
- **Detect —** the ring has not been operational for longer than T_Non_Op time. Duplicate address conditions that prevent ring operation are detected in the Detect state.
- **Non-Op-Dup —** positive indications have been received that the address of the MAC under control is a duplicate of another MAC on the ring. The ring is not operational in this state.
- **Ring-Op-Dup —** positive indications have been received that the address of the MAC under control is a duplicate of another MAC on the ring. The ring is operational in this state.
- **Directed —** the beacon process did not complete within 7 seconds; the device is sending directed beacons to notify the other stations that a serious problem exists on the ring, and a Trace state is soon to follow.
- **Trace —** a problem exists on the ring which could not be corrected during the beaconing process, and a Trace has been initiated. During a Trace, the device sends a signal that forces its nearest upstream neighbor to remove from the ring and conduct a self-test. If the ring does not recover, each subsequent upstream station will be forced to remove from the ring and conduct self-tests until the problem has been corrected.
- **? —** SPMA cannot determine the current RMT State.

TReq (Requested Target Token Rotation Time)

Displays the token rotation time bid made by the noted MAC during ring initialization, in milliseconds. T-Req is stored within the MIB in nanoseconds rather than milliseconds; SPMA converts nanoseconds to milliseconds according to the following formula:

(snmpFddiMACTReq) divided by 10^6 = T-Req msec

You can use any SNMP Set Request tool to edit the T-Req value; just remember that you must enter your value in nanoseconds, not milliseconds.

TNeg

Displays the winning token rotation time submitted by an FDDI ring station during the ring initialization, in milliseconds. The station with the lowest token rotation time bid wins the right to initialize the ring.

Current Path

Indicates which FDDI ring the noted MAC is attached to:

- **Primary —** the MAC is physically on the primary path.
- **Secondary —** the MAC is physically on the secondary path.
- **Local —** the MAC is physically on an internal local path and is not associated with the dual ring.
- **Isolated —** the MAC is not associated with any physical path.
- **? —** SPMA cannot determine the current MAC path.

Charts, Graphs, and Meters

You can view both an FDDI MAC Chart and FDDI MAC Meters (and, if you are running SPMA in conjunction with HP Network Node Manager or IBM NetView, an FDDI MAC Graph) for each available MAC entity by clicking on the appropriate buttons at the bottom of the SMT/MAC Configuration window.

NOTES

Graphing capabilities are provided by an application that is included in HP Network Node Manager and IBM NetView; therefore, graphs are only available when SPMA is run in conjunction with one of these network management platforms. If you are running SPMA in a stand-alone mode or in conjunction with SunNet Manager, no graphing capabilities are available and no graph-related options will be displayed on buttons or menus. Note that the screens displayed in this guide will include the graph-related options where they are available; please disregard these references if they do not apply.

Only general information about charts, graphs, and meters is provided in the following sections; for more detailed information, see the ***SPMA Tools Guide****.*

Viewing the FDDI MAC Chart

To view the FDDI MAC Chart window, highlight an entry in the MAC Configuration scroll list and click MAC Chart. The FDDI MAC Chart window, Figure 4-8, will appear.

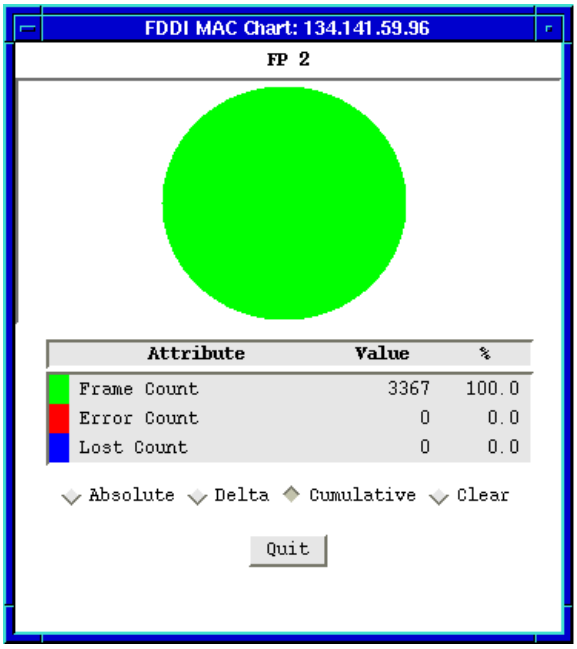


Figure 4-8. FDDI MAC Chart Window

The MAC Chart provides the following information about the selected MAC entity in both numeric and graphical form:

Frame Count

Displays the total number of frames received by the selected MAC.

Error Count

Displays a count of error frames that were detected by the selected MAC that had not been detected previously by another station. An error frame is any received frame that does not meet frame validity criteria: each frame must have a starting delimiter, a frame control field, zero or more additional data symbols, and an ending delimiter. The detecting station sets the Frame Status Error Indicator, and repeats the packet. Subsequent receiving stations do not count the frame as an error frame.

Lost Count
Displays the number of MAC PDUs (Protocol Data Units include both tokens and frames) that contain an unknown error, so their validity is in doubt. When the MAC encounters a frame of this type, it increments the Lost Frame counter and strips the remainder of the frame from the ring, replacing it with idle symbols.

Changing the Measurement of Data

Measurement fields located at the bottom of the FDDI MAC Chart window allow you to change how the incoming data is measured:

- **Absolute —** displays the chart variable values recorded in the device MIB counters.
- **Delta —** displays the difference in value for the selected data between the current poll interval and the last interval.
- **Cumulative —** displays the total since the Cumulative button was selected.
- **Clear —** resets Cumulative totals to zero; this option is not available in the Absolute or Delta modes.

To change the type of measurement, or to clear and restart Cumulative totals, click mouse button 1 on the appropriate shadowed button.

To exit the FDDI MAC Chart window, click Quit.

Viewing FDDI MAC Meters

To view the FDDI MAC Meters window, highlight an entry in the MAC Configuration scroll list and click MAC Meter. The FDDI MAC Meters window, Figure 4-9, will appear. Each of the meters provided displays a single statistic in a format that lets you know at a glance if the counter is registering high, medium, or low values.

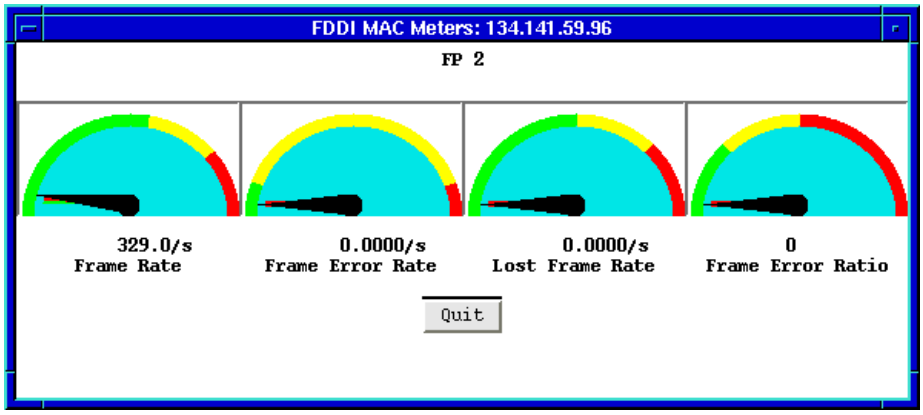


Figure 4-9. FDDI MAC Meters Window

The FDDI MAC Meters window graphically and numerically displays the following statistics:

Frame Rate

Displays the total FDDI network activity, measured in frames per second. The Frame Rate includes frames, but not tokens.

Frame Error Rate

Displays the total number of MAC Frame errors detected by the module, measured in frames per second. An error frame is any received frame that does not meet frame validity criteria: each frame must have a starting delimiter, a frame control field, zero or more additional data symbols, and an ending delimiter. The detecting station sets the Frame Status Error Indicator, and repeats the packet. Subsequent receiving stations do not count the frame as an error frame.

Lost Frame Rate

Displays the number of MAC PDUs (Protocol Data Units include both tokens and frames) that contain an unknown error, measured in frames per second. When the MAC encounters a frame of this type — whose validity is in doubt — it increments the Lost Frame counter and strips the remainder of the frame from the ring, replacing it with idle symbols.

Frame Error Ratio

Where the other meters show a snapshot of network performance, the Frame Error Ratio compares the total number of Lost and Error frames to total number of received frames, displaying a ratio which provides an overall picture of network health.

To exit the FDDI MAC Meters window, click Quit.

Viewing FDDI MAC Graphs

If you are running SPMA in conjunction with HP Network Node Manager or IBM NetView, the Port Configuration window will include a **MAC Graph** button; select this button to display FDDI variables for the selected port via the graphing application provided by your network management platform.

If you are running SPMA in conjunction with SunNet Manager or in a stand-alone mode, no graphing capabilities are available, and no graph-related options will appear.

Configuring the SMT Connection Policy

The SMT Connection Policy of an FDDI concentrator determines which types of connections are allowed among the four FDDI port types: A, B, M (Master), and S (Slave). FDDI protocol forbids Master—>Master connections; all other connection types are legal, although some are considered to be undesirable.

To open the SMT Connection Policy window:

from the Hub View:

1. Click either mouse button on any Module Index or Module Type text box to display the Module Menu (remember, this menu is the same for all application display modes).
2. Drag down to **FDDI Utilities**, then across to select **SMT Connection Policy**.

from the command line (stand-alone mode):

1. From the appropriate directory type:

```
spmarun fddicpol <IP Address> <community name>
```

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from within the Hub View.*

*If you wish to configure the connection policy, be sure to use a **community name** with at least Read/Write access. If you only wish to view the policy, a community name with Read access will be sufficient.*

*If there is a hostname mapped to your 7C0x's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is not the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

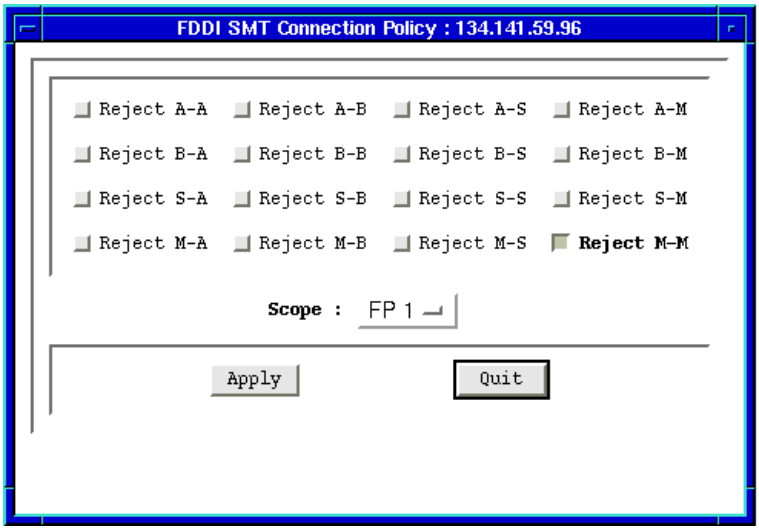


Figure 4-10. SMT Connection Policy Window

FDDI Connection Rules

By default, all connections are allowed except the illegal **M—>M** connection; the following table summarizes the FDDI connection rules:

Table 4-1. FDDI Connection Rules

	A	B	S	M
A	V, U (T)	V	V, U	V, DH
B	V	V, U (T)	V, U	V, DH
S	V, U	V, U	V	V
M	V, DH	V, DH	V	X

V — valid connection
X — illegal connection
U — undesirable (but legal) connection
T — connection can lead to a twisted ring configuration
DH — when both A and B are connected to M ports, a dual-homing configuration results. See the following page for more information on dual homing.

CAUTION

Though technically legal under FDDI connection rules, the undesirable A—>S and B—>S connections will deprive your device of the redundancy protection built in to the FDDI dual-ring configuration. The SMT entity is notified each time an undesirable connection is made, even when that connection is allowed.

Each interface controls only its own connection policy; however, when two interfaces attempt to connect, their *combined* connection policies dictate the connections that will be allowed, with the most lenient policy prevailing — in other words, all connections (except for the illegal M—>M connection) are allowed unless forbidden by *both* connecting nodes. For example, if you disallow the A—>M connection on one node, but attempt to make that connection with another node which does not forbid it, the connection will be allowed.

Special Ring Configurations

You can use the SMT Connection Policy window to allow or prevent the following ring configurations:

Dual Homing

Dual homing is a method of configuring concentrators with a redundant topology that provides a backup data path to protect critical devices from losing contact with the main ring; dual homing also achieves a kind of separation from the main ring that makes it easy to bring a critical device down for maintenance without causing widespread ring failure.

To achieve a dual homing configuration, connect the A port of your critical device to an M port on one dual-attached concentrator (DAC), and connect the B port of the same device to an M port on another DAC. SMT will automatically make the B—>M connection active and place the A—>M connection in stand-by; the A—>M connection will only become active if the B—>M connection should fail. (Once the B—>M connection is restored, it is automatically re-activated, and the A—>M connection goes back into standby mode.) Dual homing will not be permitted if either the A—>M or B—>M connections have been disallowed for all involved nodes.

Twisted Ring

When an FDDI ring is in a twisted configuration, at least one station is supporting ***both*** an A—>A connection and a B—>B connection; in this configuration, the station with the A—>A and B—>B connections is actually residing on the secondary FDDI ring, and is therefore isolated from the stations on the primary ring. A wrap condition on a twisted ring will bring the isolated station back into contact with any stations still connected to the primary ring. You can prevent a twisted ring configuration by disallowing the A—>A and/or the B—>B connections for all nodes.

Defining Your Connection Policy

To configure the connection policy for the selected interface:

1. To disallow any connection types, click mouse button 1 on the appropriate selection box or boxes; to allow connections which have been previously disallowed (except for the illegal **M—>M** connection), click on the selection box again.

2. In the **Scope** field, click on the selection button to select the front panel interface (FP) or SMT entity for which you wish to configure connection policy. (Remember, if you launch from the command line, front panel designations will not appear, and each interface will be indexed by SMT only.) Changes will only be applied to those ports associated with the front panel interface or SMT entity which is listed in the **Scope** field when Apply is selected.
3. Click on Apply to put your policy into effect.
4. To make changes to the connection policy for additional front panel interfaces or SMT entities, change the selection in the **Scope** field, reject or allow connections as desired, then click on Apply again.

Viewing the Station List

Selecting the Station List option from the FDDI Utilities menu allows you to view a list that shows all the stations on the FDDI ring to which the selected interface is attached, along with some general information about each station.

To access the Station List window (Figure 4-11):

from the Hub View:

1. Click either mouse button on any Module Index or Module Type text box to display the Module Menu (remember, this menu is the same for all application display modes).
2. Drag down to **FDDI Utilities**, then across to select **Station List**.

from the command line (stand-alone mode):

1. From the appropriate directory type:

```
spmarun fddislst <IP Address> <community name>
```

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from within the Hub View.*

*A **community name** with Read access is sufficient to view the station list.*

*If there is a hostname mapped to your 7C0x's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is not the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

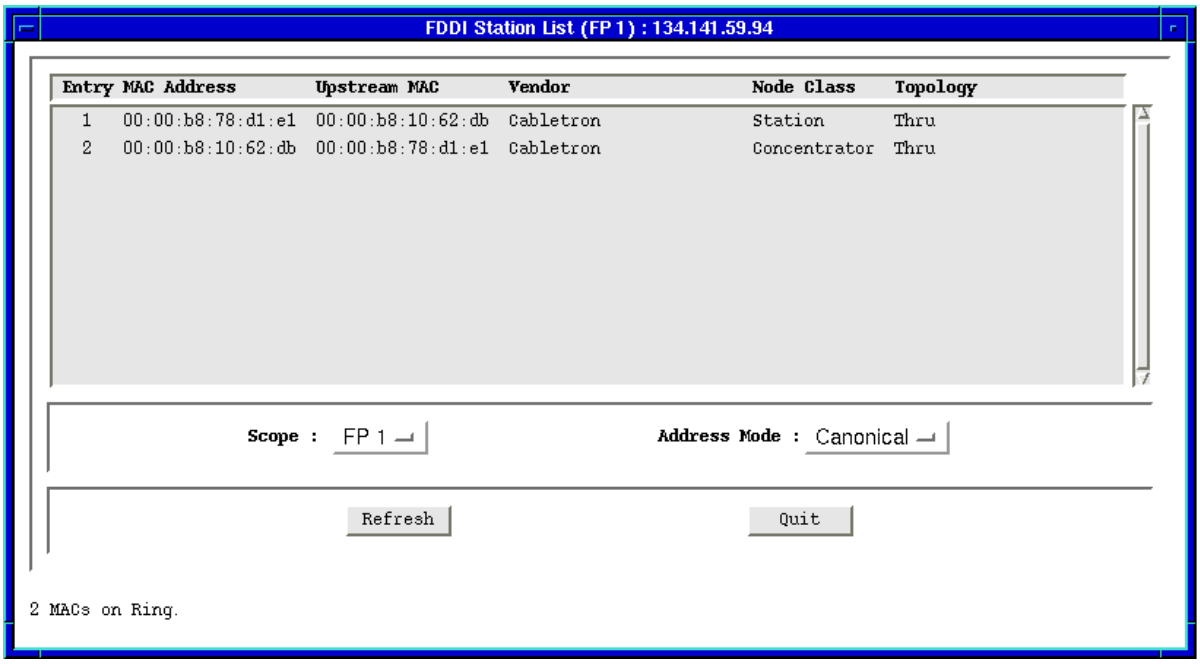


Figure 4-11. The Station List Window

Note that the information displayed in the Station List window is static once the window is opened; for updated information, click mouse button 1 on Refresh. Also, note the scroll bar located to the right of the list window; use it to view additional stations, if necessary. The total number of MAC entities (which may or may not equal the number of devices or stations) on the listed ring is displayed at the bottom of the window.

The Station List window provides the following information about each node residing on the same ring as the front panel interface or SMT entity selected in the **Scope** field, beginning with the selected interface and traveling upstream. (Remember, if you launch the Station List application from the command line, no front panel designations will appear; each FDDI interface will be listed by its SMT index only.)

Entry

An index number assigned to each station in the ring. The front panel interface or SMT entity currently selected in the **Scope** field is always assigned number one.

MAC Address

The MAC, or hardware, address of each station on the ring. You can display the MAC address in Canonical (FDDI) format or MSB (Ethernet) format by clicking mouse button 1 on Canonical, then dragging down to select the desired address mode. The **Address Mode** field above the button displays the current setting; the default display mode is Canonical (FDDI).

Upstream MAC

Displays the hardware address of the node's nearest upstream neighbor. Note that the addresses displayed in this field also respond to any change in display mode from MSB to Canonical, or vice versa.

Vendor

Displays the name of the vendor that manufactured the device, as determined by the first three bytes of the MAC address.

Node Class

Indicates the node type: either station or concentrator.

Topology

Indicates the node's current MAC configuration topology; possible states are:

Thru	The ring is operating normally, with no cable breaks or bad nodes directly upstream or downstream of the selected node: the primary path enters the A port and emerges from the B port, and is currently active; the secondary path enters the B port and emerges from the A port, and is not currently in use.
Wrapped	The node is wrapped, due to a cable break, a bad station, or management action; the secondary path has been wrapped into the primary path to restore the ring.
Isolated	The node is isolated from the ring; a node in this state will be the only one displaying in the station list.
A-A Twisted	The ring is in a twisted configuration, because the node's A port has been connected to another A; by necessity, somewhere on the ring a B port is connected to another B, and a third station has both an A—>A *and* a B—>B connection. The ring can operate normally in a twisted condition, but the station with both an A—>A and B—>B connection is isolated from the primary ring and residing alone on the secondary ring.
A-A Twisted, Wrapped	The ring is twisted due to an A—>A connection on this node, as described above; the ring is also wrapped. Note that the wrap condition brings the node with both the A—>A *and* B—>B connection back into contact with the rest of the stations on the ring, since the secondary ring has become part of the primary ring.
B-B Twisted	The ring is in a twisted configuration, because the node's B port has been connected to another B; again, by necessity, somewhere on the ring an A port has been connected to another A, and a third station has both and A—>A *and* a B—>B connection. The ring can operate

	normally in a twisted condition, but the station with both an A—>A and B—>B connection is isolated from the primary ring and residing alone on the secondary ring.
B-B Twisted, Wrapped	The ring is twisted due to the node's B—>B connection, as above; in addition, the ring is wrapped, bringing any node isolated by the twist back into contact with the stations on the main ring.
Unknown	SPMA is unable to determine the node's topology state.

Chapter 5

ATM Configuration

Configuring Permanent Virtual Circuits (PVCs); adding and deleting connection entries

The ATM interface available via the 7A06-01 NIM module provides the connectivity that allows you to merge ATM network segments with traditional LAN technologies via the SmartSwitch chassis backplane. Current versions of 7A06-01 firmware use 802.3 VC-based multiplexing for bridging protocols to move PVC traffic between the ATM front panel connection and the SmartSwitch backplane; future versions will add support for ATM Forum LAN Emulation and Cabletron's SecureFast switching.

An ATM network uses two types of virtual channels, or circuits: Switched Virtual Circuits, or SVCs, and Permanent Virtual Circuits, or PVCs. SVCs are created and dismantled dynamically on an as-needed basis, and require no management definition; PVCs, however, must be manually configured. The AToM MIB window provides the means for accomplishing these configurations.

Accessing the AToM MIB Window

To access the AToM MIB window

from the Hub View:

1. Click either mouse button on any Module Index or Module Type text box to display the Module Menu (remember, this menu is the same for all application display modes).
2. Drag down to **ATM**, and release.

from the command line (stand-alone mode):

1. From the appropriate directory type:

```
spmarun atmcfg <IP Address> <community name>
```

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from within the Hub View.*

*If you wish to configure or delete any PVCs from the AToM MIB window, be sure to use a **community name** with at least Read/Write access. If you only wish to view configured PVCs, a community name with Read access will be sufficient.*

*If there is a hostname mapped to your 7C0x's IP address, you can use **<hostname>** in place of **<IP address>** to launch this application. Please note, however, that the hostname is not the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

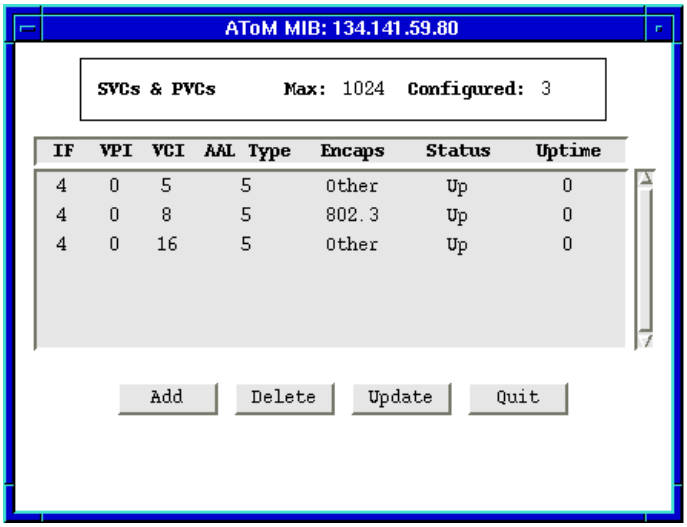


Figure 5-1. The AToM MIB Window

The AToM MIB window provides the following information about the ATM connections configured for any installed 7A06-01 interfaces:

TIP

Each 7A06-01 NIM provides two ATM interfaces; these are intended to serve as redundant interfaces, and only one may be active at a time. However, any change in the active interface will be transparent to the ATM application and requires no additional configuration; both interfaces share an IF index and all ATM configuration settings.

Max

Displays the maximum number of connections (both SVCs and PVCs) allowed by current device firmware.

Configured

Displays the number of connections (both SVCs and PVCs) currently configured.

The remainder of the window contains a list box which displays the following information about each of the currently configured PVCs; use the scroll bar to the right of the list to view additional connections, if necessary:

Interface

The device interface on which the PVC was configured. Index numbers are assigned in an XXXXYY format, where X = slot index times 10,000, and Y = port index; note that the redundant interfaces on each 7A06-01 NIM share a single IF index, and changes in the active interface will be transparent to this window.

VPI

Displays the Virtual Path Identifier assigned to the connection; current versions of 7A06-01 firmware allow values from 0–3. Virtual Path Identifiers are used to group virtual connections, allowing for channel trunking between ATM switches. Each VPI can be configured to carry many different channels (designated by VCIs) between two points.

VCI

Displays the Virtual Channel Identifier assigned to the connection; allowable values are 0–1023 *for each VPI*. Each assigned VCI must be unique within its defined VPI: for example, you can assign a VCI of 14 as many as four times: once with a VPI of 0, once with a VPI of 1, and so on. Remember, it is the combined VPI and VCI designations assigned to a channel that creates the grouping of virtual connections.

AAL Type

This field indicates which AAL protocol type is currently in use on the Virtual Channel Circuit (VCC). An instance of this object only exists when the local VCL end-point is also the VCC end-point, and the ATM Adaptation Layer (AAL) is in use. The ATM Adaptation Layer maps user, control, and management data into or out of the information field of ATM cells of a virtual connection. The possible Protocol Type Values are:

- **1** (AAL1) — this protocol is used in Constant Bit Rate (CBR) services, which require information to be transferred at a constant rate after the virtual connection has been established.
- **34** (AAL3/4) — the protocol used for connectionless or connection-oriented transfer of data which may be sensitive to loss but not to delay.
- **5** (AAL5) — the protocol used for connection-oriented data transfer that requires better error detection than available with AAL 3/4. (Note, however, that the AAL5 protocol itself does not support multiplexing.)
- **other —** which may indicate a user-defined AAL type.
- **unknown —** which indicates that the AAL type cannot be determined.

Encaps
Displays the method used to encapsulate LAN packets on the selected circuit. Current versions of 7A06-01 firmware use 802.3 VC-based multiplexing for bridging protocols (designated **802.3**); future versions will add support for ATM Forum LAN Emulation and Cabletron's SecureFast Switching.

Status
Displays the current administrative status of the connection: Up (enabled) or Down (disabled). In current versions of firmware, all connections are enabled by default, and cannot be disabled.

Uptime
The length of time the selected connection has been enabled. This field is not currently supported by firmware, and will display only a value of 0.

Add
Selecting the **Add** button launches the Create Channel window, which allows you to configure additional PVCs.

Delete
Selecting the **Delete** button deletes the selected connection.

Update
Selecting **Update** refreshes the connection information displayed in the list box.

Configuring Connections

To configure new Permanent Virtual Circuits (PVCs):

1. From the AToM Mib window, click to select Add. The Create Channel window, Figure 5-2, will appear.

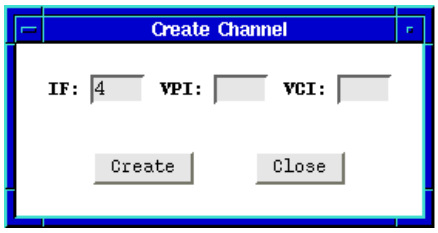


Figure 5-2. The ATM Create Channel Window

2. The **Interface** text box will by default display the index number assigned to the active ATM front panel interface whose connection was selected in the AToM MIB window. If you have more than one 7A06-01 installed in your

SmartSwitch chassis, use this field to enter the interface number for which you wish to configure a new circuit. (Remember, each pair of redundant interfaces shares a single IF index.)

3. In the **VPI** text box, enter the Virtual Path Identifier you wish to assign to this connection. Allowable values are 0 to 3; remember, the VPI you assign will be used to group virtual connections, allowing for channel trunking between ATM switches.

4. In the **VCI** text box, enter the Virtual Channel Identifier you wish to assign to this connection. Allowable values are 0 to 1023 *for each VPI*. For example, you could assign the same channel identifier — say, 25 — as many as four times: once with a VPI of 0, once with a VPI of 1, and so on. Again, remember that it is the combination of VPI and VCI that will be used to direct cells through the intermediate switches between the source and destination.

5. Click Create to add the new permanent circuit to the ATM interface. This circuit will remain in place until it is manually removed using the Delete option in the Current Connections window.

Chapter 6

Using the 7C0x SmartSwitch Bridge View

A brief explanation of bridging methods; a tour of the Bridge Traffic View; using the Detail View; monitoring bridge operation; using the Filtering Database; configuring bridge operating parameters; setting forwarding thresholds, statistics, and notification options; setting polling parameters; enabling and disabling bridge interfaces

---

The SPECTRUM Portable Management Application (SPMA) Bridge View presents a series of windows that describe the bridging services available via the modules installed in your 7C0x SmartSwitch chassis. You can monitor bridge activity and performance and manage bridge configuration through the Bridge Traffic View and other related windows.

Bridging Basics

Bridges are used in local area networks to connect two or more network segments and to control the flow of packets between the segments. Ideally, bridges forward packets to another network segment only when necessary. Bridges are also used to increase the fault tolerance in a local area network by creating redundant bridge paths between network segments. This is so that in the event of a bridge or bridge segment failure, an alternate bridge path will be available to network traffic, without significant interruption to its flow.

The method a bridge uses to forward packets, choose a bridge path, and ensure that a sending station's messages take only one bridge path depends on the bridge's type: Transparent or Source Routing. This chapter describes viewing and configuration options related to Transparent bridges.

TIP

Source route bridging is not yet supported for the 7C0x SmartSwitch, as no Token Ring NIMs are currently available.

Transparent Bridging

Transparent bridges are most common in Ethernet networks. Individual Transparent bridges monitor packet traffic on attached network segments to learn their network segment location in terms of which bridge port receives packets originating from a particular station (determined via the packet's Source Address field). This information gets stored in the bridge's Filtering Database. When in the Forwarding state, the bridge compares a packet's destination address to the information in the Filtering Database to determine if the packet should be forwarded to another network segment, or filtered (i.e., not forwarded). A bridge filters a packet if it determines that the packet's destination address exists on the same side of the bridge as the source address.

Transparent bridges in a network communicate with one another by exchanging Bridge Protocol Data Units, or BPDUs, and collectively implement a Spanning Tree Algorithm (STA) to determine the network topology, to ensure that only a single data route exists between any two end stations, and to ensure that the topology information remains current.

Accessing the Bridge Traffic View Window

There are three ways to open the Bridge View: if you are working within a network management system, you can select the **Bridge View** option from the icon menu; specific directions for creating a 7C0x SmartSwitch icon and accessing the icon menu can be found in the appropriate ***Installing and Using SPECTRUM for...*** guide. If you are using the Hub View, you can select the **Bridge Mgmt** option from the Bridge menu (available only in Bridge Application Display mode); or, if you are running in a stand-alone mode, type the following at the command line:

```
spmarun bridge <IP address> <community name>
```

NOTES

*The **spmarun** script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from the icon menu or from within the Bridge Traffic View.*

*If there is a hostname mapped to your bridging device's IP address, you can use <hostname> in place of <IP address> to launch the Bridge View. Please note, however, that the hostname is **not** the same as the device name which can be assigned via Local Management and/or SPMA; you cannot use the device name in place of the IP address.*

The community name you use to start the Bridge application must have at least **Read** access; for full management functionality, you should use a community name that provides **Read/Write** or **Superuser** access. For more information on community names, consult the appropriate ***Installing and Using SPECTRUM for...*** guide, and/or the **Community Names** chapter in the ***SPMA Tools Guide.***

The Bridge Traffic View is the heart of the Bridge application. The first window to appear when you start the Bridge application, it contains a status display of the device's bridge ports and contains the buttons and menus that provide access to all bridge monitoring and management functions.

Navigating Through the Bridge Traffic View

Within the Bridge Traffic View, you can click mouse buttons in different areas of the window to initiate management tasks. The following diagram shows you how to display the Bridge Traffic View Device and Port menus.

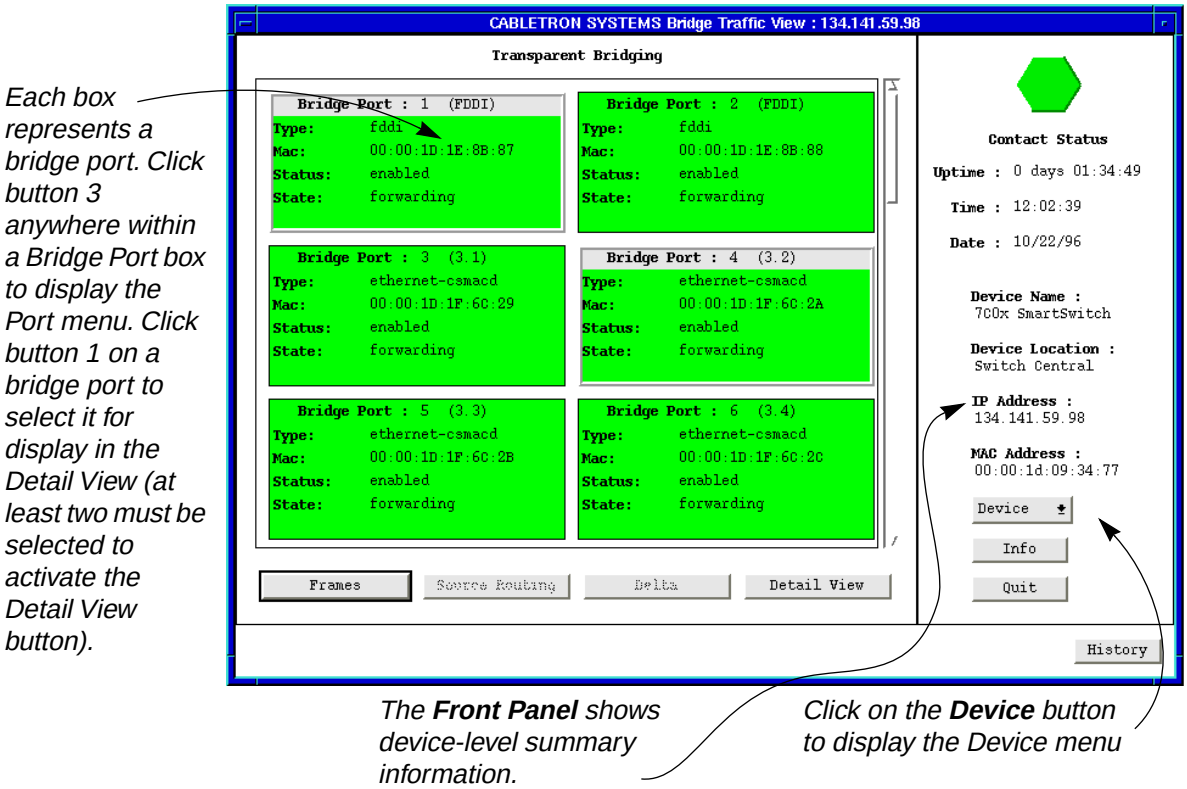


Figure 6-1. Mousing Around the Bridge Traffic View

To display the Device menu:

1. Click on Device in the Bridge Traffic View front panel.

To display a Port menu:

1. Click mouse button 3 in a Bridge Port box.

Bridge Traffic View Front Panel

The right side of the Bridge Traffic View displays device summary information:

Contact Status

Contact Status is a color code that shows the status of the connection between SPMA and the device:

- Green means a valid connection.
- Blue means that SPMA is trying to reach the device but doesn't yet know if the connection will be successful.
- Red means that SPMA has lost contact with the device.

Uptime

The time that the device has been running without interruption. The counter resets to 0 days 00:00:00 (X days HH:MM:SS) when one of the following occurs:

- Power to the device is cycled.
- The device is reset manually.

Time and Date

The date and time are taken from the device's internal 24-hour clock, which you can set in the Bridge Status window; see **The Bridge Status Window**, page 6-11.

Device Name

This field displays the name you've assigned to this device in the Bridge Status window; see **The Bridge Status Window**, page 6-11.

Device Location

This field displays the location you've assigned to this device in the Bridge Status window; see **The Bridge Status Window**, page 6-11.

NOTE

If you have assigned a device name or location that contains more than 18 characters, only the first 18 will be displayed in the Bridge Traffic View. Check the Device Status window for the complete name and/or location, if necessary.

IP Address

The device's Internet Protocol address. You cannot change the IP address from SPMA. For multi-interface devices which support multiple IP addresses, this will be the IP used to define the device icon (if you are using a management platform) or the IP used to launch the application (if you are running in stand-alone mode).

MAC Address

The factory-set MAC hardware address assigned to me 7X00 Controller module's backplane (or Host) interfaces. (Note that these two internal interfaces share a MAC address.)

Device

Clicking on the **Device** button displays the Device menu. The Device menu lets you perform the following:

- Open the Bridge Status window
- Display a summary of bridge statistics
- Open the Filtering Database window
- Open the Find MAC Address window
- Open the Special Database window
- Open the Spanning Tree Protocol window
- Open the Polling Intervals window

Info

If you need to call Cabletron's Technical Support about a problem with the Bridge View, you'll need the information provided in the Information window:

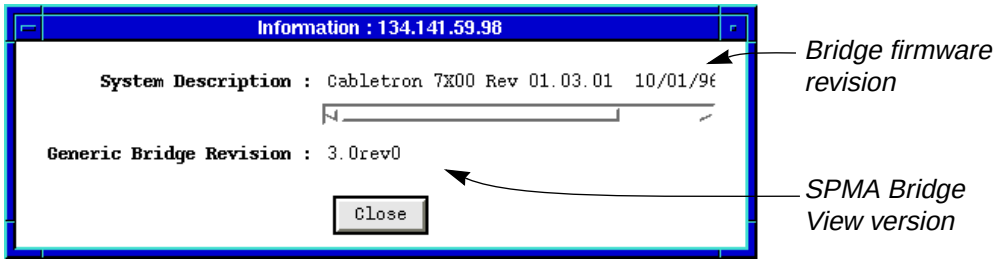


Figure 6-2. Bridge Information Window

Quit

Clicking mouse button 1 on the Bridge Traffic View **Quit** button closes all Bridge View windows.

The Bridge Port Display

Each Bridge Port box in the Bridge Traffic View displays information about its corresponding bridge port.

The Bridge Port boxes are color-coded, reflecting their current status. Bridge Port boxes for disabled bridge ports are colored blue. Enabled bridge ports are colored green, yellow, or red, depending on the range in which the traffic volume through that port falls. See **Configuring Forwarding Thresholds**, page 6-30, for complete instructions on assigning traffic ranges and their corresponding Bridge Port box colors.

Bridge Port box fields are as follows:

Port

The index number assigned to the bridge port.

Type

The bridge port's interface type (e.g. ethernet-csmacd, fddi, ppp, token ring, etc.).

MAC

The MAC address of the interface associated with the port.

The remaining information displayed in the Bridge Port boxes depends on selections made using the buttons located at the bottom of the Bridge Traffic View. See the next section, **Choosing Bridge Traffic Information: Bridge Traffic View Buttons**, for instructions on using these buttons.

Choosing Bridge Traffic Information: Bridge Traffic View Buttons

The four buttons at the bottom of the Bridge Traffic View control the type of information that appears in some of the Bridge Port box fields. (The Port number, Type, and MAC address fields are not affected by any of these buttons.)

The **Frames/Admin**, **Source Routing/Transparent**, and **Delta/Percentage** buttons each let you choose one of the two display modes for the Bridge Port boxes. The display mode visible on a button is the one ***not*** currently selected. Clicking on a button when the button displays the desired mode type chooses that mode type for the Bridge Port boxes. For example, the **Frames/Admin** button will display **Frames** when the Admin display mode is in effect and **Admin** when the **Frames** display mode is in effect.

The **Frames/Admin** button allows you to change the information displayed in the Bridge Port boxes between traffic statistics (when **Frames** is selected) and port state/status (when **Admin** is selected).

The Frames display mode shows the following Bridge Port information:

- **Frms In**—Displays the total number of frames, including BPDU frames, received at this bridge port from its attached network segment during the last polling interval.
- **Frms Out**—Displays the total number of frames, including BPDU frames, transmitted or forwarded through this port to its attached network segment during the last polling interval.
- **Forwarded**—Displays frames forwarded by this bridge port to another bridge port on the device during the last polling interval. You can change this display using the **Delta/Percentage** button (described in this section). When **Delta** is selected, this field displays the total number of frames forwarded by this bridge port to another port on the bridge during the last polling interval. When **Percentage** is selected, this field displays the percentage of all frames received by the port from its network segment that were forwarded to another port on the bridge during the last polling interval.

When the Admin option is selected, the Bridge Port boxes display port **Status** —whether the port is enabled or disabled — and port **State**.

Enabled	The port is able to participate in bridging and the Spanning Tree Algorithm.
Disabled	The port cannot participate in bridging or Spanning Tree operations.

A port's State indicates whether or not the port is forwarding packets and participating in the exchange of BPDUs. The Spanning Tree Algorithm determines the state of each port in order to maintain an active topology with no data loops. As a port moves from the blocking to the forwarding state, it will remain in each state for the duration of the Forward Delay in order to prevent data loops while the active topology is changing. Possible port states are as follows:

Disabled	The port has been disabled by management; it cannot receive or forward traffic, and is not participating in the exchange of BPDUs.
Blocking	This port is not forwarding or receiving traffic (and therefore no physical address information is added to the Filtering Database), but it will still send out and receive BPDUs. A port will enter the blocking state for two reasons: if it receives information that another bridge is the designated bridge to the network segment to which this port is attached, or immediately after it has been enabled by management.
Listening	This state is entered from the blocking state when the STA determines that this port should participate in frame relay. The port is processing BPDUs, but is not yet forwarding or receiving traffic or adding information to the Filtering Database.

Learning	The port is processing BPDUs, but is not yet relaying packets. The port is adding address information to the Filtering Database.
Forwarding	A port enters this state from the Learning state. The port is relaying frames and processing BPDUs. A port in this state can enter the Disabled state via by management action.
Broken	If the port is malfunctioning, this value will display in the State field.

Source Routing | Transparent

This button is grayed out because the 7C0x SmartSwitch currently performs Transparent bridging only (since no Token Ring NIMs are yet available). The title bar at the top of the Bridge Port display area indicates the frame type described in the bridge ports.

Delta | Percentage

This two-state button is active when you have bridge statistics displayed in the Bridge Port boxes (i.e., when **Frames** is selected); otherwise, it is grayed. When you click on **Delta**, the **Forward** field in the Bridge Port boxes displays the total number of frames forwarded by this bridge port to another port on the bridge during the last polling interval. When you click on **Percentage**, the **Forward** field in the Bridge Port boxes displays the percentage of all frames received by the port from its network segment that were also forwarded to another port on the bridge during the last polling interval.

Detail View

The **Detail View** button lets you take a closer look at traffic between two, three, or four selected bridge ports. The **Detail View** button is grayed unless you have at least two bridge ports selected. For complete instructions on how to use the Detail View, see the next section.

Using the Detail View Window

The Detail View provides port-level information on any two, three, or four ports. To open the Detail View:

1. In the Bridge Traffic View, select two, three, or four ports by clicking mouse button 1 on the desired ports; the selected Port boxes will be outlined, and the top part of each selected box will be grayed. The **Detail View** button becomes active once you select at least two bridge ports.
2. Click on the **Detail View** button. The Detail View window appears.

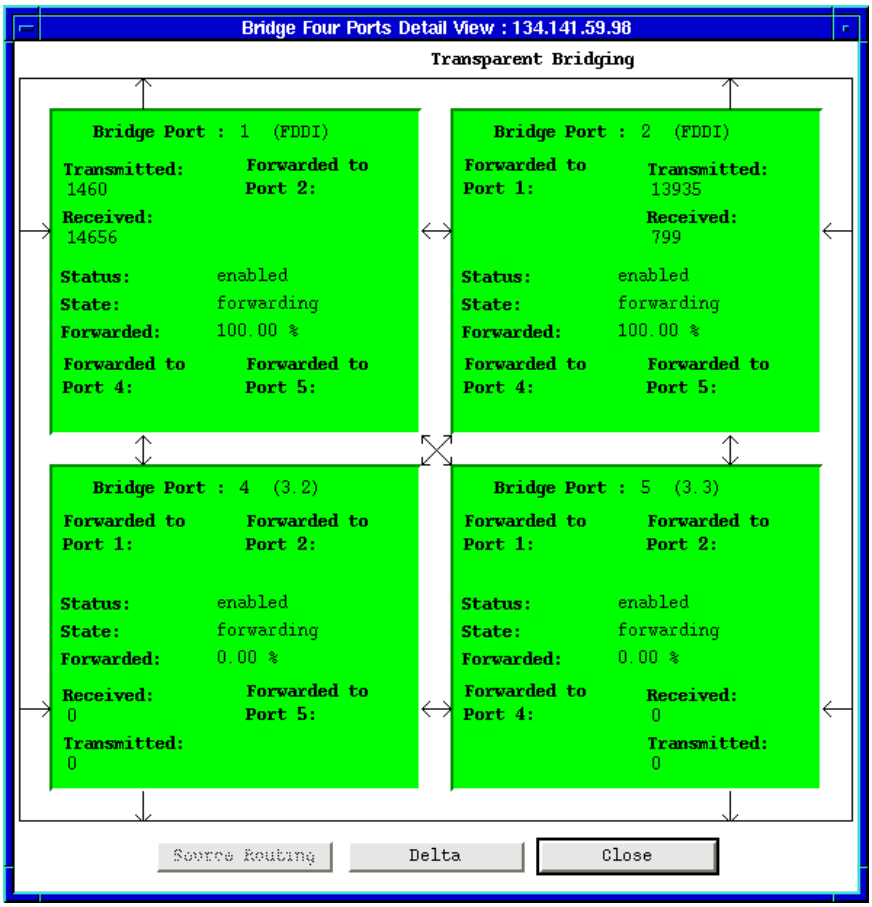


Figure 6-3. Detail View Showing Four Ports

Each port shows the total frames transmitted and received by the port.

Port summary information includes Port Index (at the top of the Bridge Port box), Port Status, Bridge Port State, and Frames Forwarded. You can display Frames Forwarded as a delta value (the total number of frames forwarded by this bridge port to any other port on the bridge during the last polling interval) or as a percentage value (showing the percentage of all frames received by the port from its attached network segment during the last polling interval that were forwarded to another port on the bridge) by clicking the Delta/Percentage button at the bottom of the window (see Figure 6-3).

Each corner of the bridge port summarizes activity to another bridge port. You can display Forwarded To as a delta value (the total number of frames forwarded by this bridge port to the specified port on the bridge during the last polling interval) or as a percentage value (showing the percentage of all frames received by the port during the last polling interval that were forwarded to the specified port on the bridge) by clicking the Delta/Percentage button at the bottom of the window (see Figure 6-3).

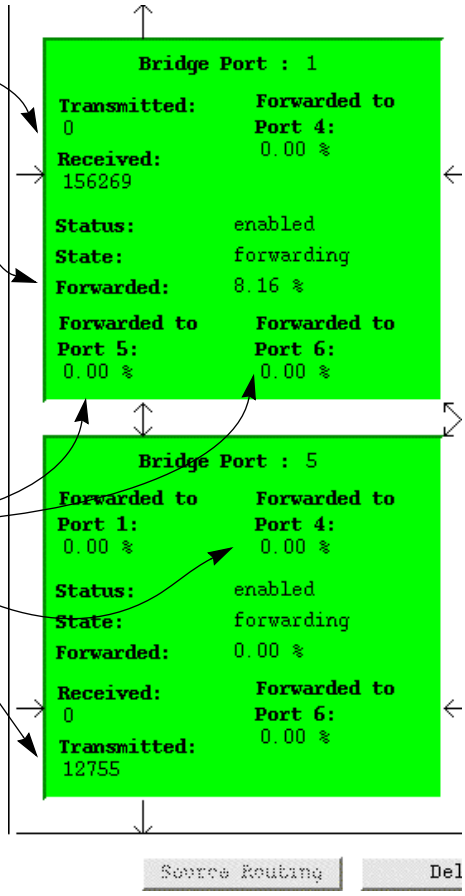


Figure 6-4. Port Boxes in the Detail View

Changing Ports in the Detail View

The Detail View can display up to four ports at the same time. If the bridge has more than four ports, you can show other device ports by exchanging an existing port in the Detail View for a port that is not displayed.

To select a new port for the Detail View:

1. In the Detail View, click mouse button 3 on the bridge port you want to replace with another port. The **Change Menu** appears.
2. Select the range of bridge ports (e.g., **Port 1-10**) that includes the desired port. A menu listing the individual ports included in the selected range (i.e., **Port 1**, **Port 2**, **Port 3**, and so on) will appear. Ports that are currently displayed in the Detail View are grayed in the menu.
3. Select the desired Bridge Port index number from the list. The port box will display information for the newly selected port.

The Bridge Status Window

You can set or change the device time, date, name, or location—all of which display in the Bridge Traffic View Front Panel—in the Bridge Status window.

The **Contact** field is the only Bridge Status window field not displayed in the Bridge Traffic View Front Panel. Use the Contact box to record the name and phone number of the person responsible for the device.

To set or change information for any of the Bridge Status window fields:

1. Display the Device menu by clicking on the Front Panel Device button.
2. In the Device menu, drag down to **Status** and release.
3. In the Status window, highlight a text box, type in the new information; press **Enter** or **Return** on the keyboard to set your changes before selecting a new field.

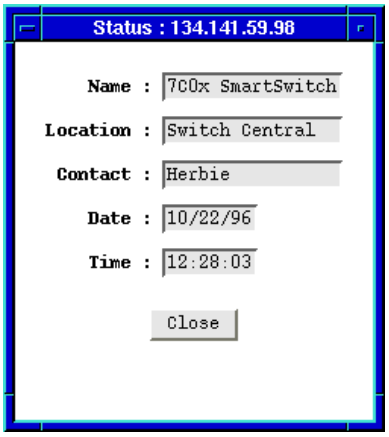


Figure 6-5. Bridge Status Window

The Bridge Statistics Window

The Bridge Statistics window displays generic information about all ports associated with the device.

To open the Bridge Statistics window:

1. In the Bridge Traffic View window, click on Device to display the Device menu.
2. Drag down to **Bridge Statistics** and release. The Bridge Statistics window appears.

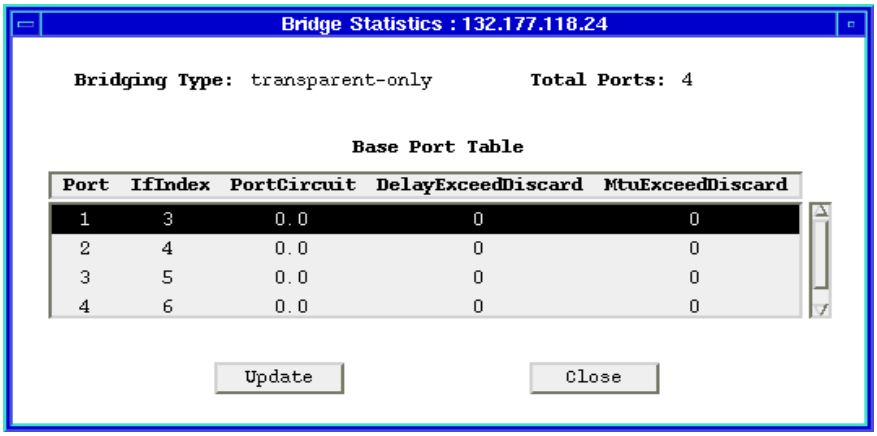


Figure 6-6. Bridge Statistics Window

The Bridge Statistics window displays the following information:

Bridging Type

Type refers to the type of bridging supported by the bridge.

- unknown
- transparent-only

Total Ports

Shows the total number of bridge ports installed in the 7C0x SmartSwitch chassis.

Port

Displays each port's index number.

IfIndex

Interface index; a unique value for each network (interface) to which this port connects. Only a WAN port will connect to more than one interface simultaneously.

PortCircuit

When dealing with X.25 virtual circuits, it's possible for two Port Indexes to have the same IfIndex. In such a case, Port Circuit contains the value of a MIB object instance unique to the port; otherwise, Port Circuit is equal to 0.0. For example, if Port 1 maps to IfIndex 1 and Port 2 maps to Ifindex 1, then the Port Circuits are 1.1 and 1.2 respectively.

DelayExceedDiscard

The number of frames a port has discarded due to an excessive transit time through the bridge.

MtuExceedDiscard
Mtu stands for "maximum transfer unit"; it is the largest frame size that can be processed by the 7C0x SmartSwitch. A port discards any received frames that are larger than the Mtu; this field lists how many such frames were discarded.

Update

The information in the Bridge Statistics window is a snapshot of the data. When you open the Bridge Statistics window, the application polls the devices for information. Devices are not polled again until you click mouse button 1 on the **Update** button, or close, then re-open the Statistics window.

NOTE

When a device is reset, statistics windows and/or statistics displays in the Bridge View windows may display very large numbers for one polling interval. This is due to the resetting of counters.

The Filtering Database Window

In Transparent bridging, each bridge port uses the device's Filtering Database to determine a packet's route through the bridge. The Filtering Database is created from permanent entries made via management, and from entries learned as the bridge collects and stores the source address and port association from each packet it receives.

When in the Forwarding state, the bridge examines each received packet and compares the destination address to the contents of the Filtering Database. If the destination address is located on the network from which the packet was received, the bridge filters (does not forward) the packet. If the destination address is located on a different network, the bridge forwards the packet to the appropriate network. If the destination address isn't found in the Filtering Database, the bridge forwards the packet to all networks. To keep Filtering Database entries current, older entries are purged after a period of time, which is called the Dynamic Ageing Time.

The Filtering Database has two types of entries: Forwarding and Static. The Forwarding view of the Filtering Database contain addresses that the bridge learns from network traffic (also known as dynamic entries) as well as all the static entries. Learned entries are subject to the bridge's Dynamic Ageing Timer; entries that aren't accessed within the time specified by the ageing timer are purged. Static entries may be subject to the ageing timer, depending on how the entries were added. Static entries enter the Filtering Database in two ways: either automatically, when permanent database entries are copied to the Filtering Database, or manually when you move a Forwarding entry to the Static Table.

Viewing the Filtering Database

To open the Filtering Database window:

1. Display the Device menu by clicking on the Front Panel Device button.
2. Drag down to **Filtering Database**, and release.
3. At the top of the Filtering Database window, click mouse button 1 on the appropriate selection box to view either the **Forwarding** or **Static** database.

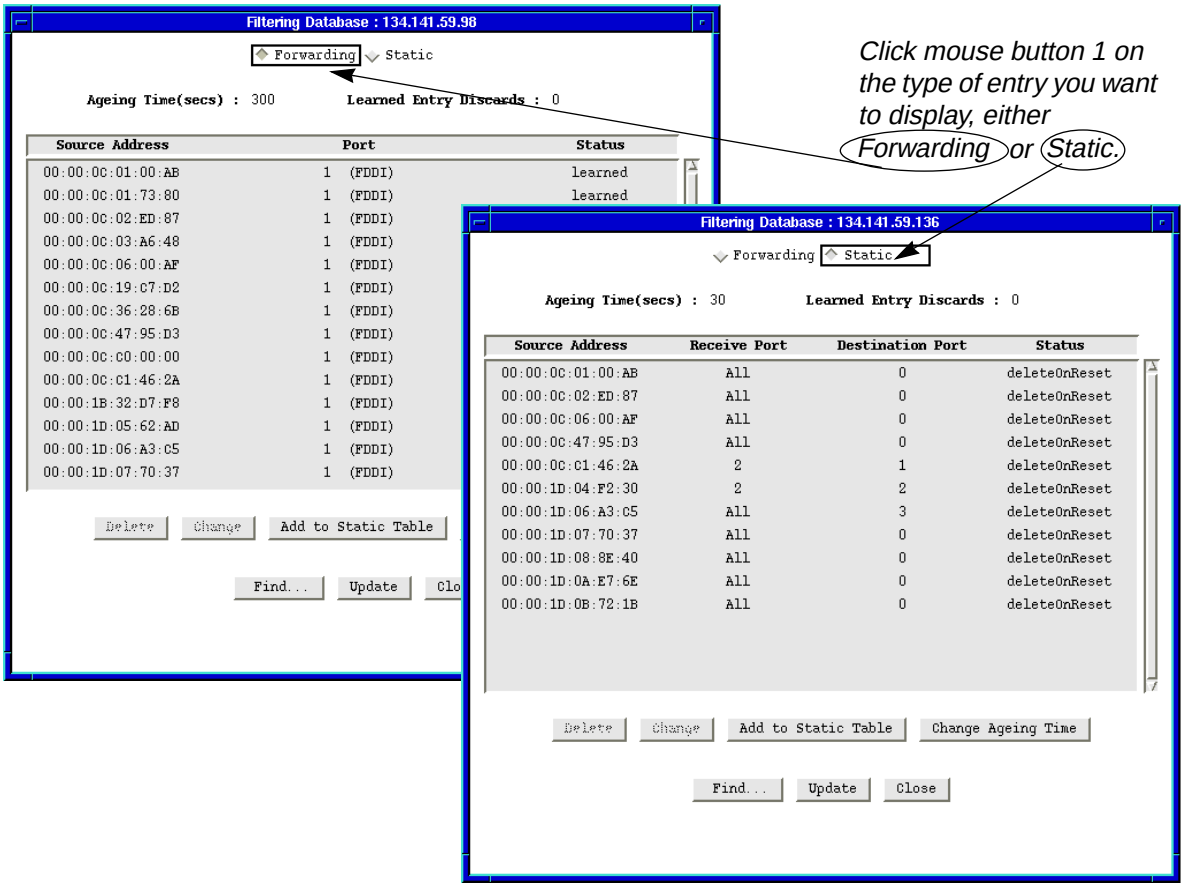


Figure 6-7. Filtering Database Window

Two fields at the top of the Filtering Database window provide information about the Filtering Database:

Ageing Time (secs)

The current setting of the bridge's Dynamic Ageing Timer, used to purge Forwarding entries from the Filtering Database, or to purge static entries subject to the ageing timer.

Learned Entry Discards

The number of database entries that never made it into the Filtering Database due to a lack of buffer space. Ideally, this number should be 0. If this number grows, it indicates a very busy network. A value other than 0 is acceptable as long as it isn't increasing, indicating that the lack of buffer space is sometimes causing problems, but that the condition is not persistent.

For each entry in the Forwarding database, the window displays the following:

Source Address

Displays the MAC addresses of devices that have transmitted frames to the bridge.

Port

Identifies the bridge port where frames from the noted source address are received. A value of 0 indicates that the address exists within the Filtering Database, but the database has not yet learned the corresponding port number.

Status

Indicates how the entry got into the database:

- **learned**—The address was copied into the database from the source address field of a received frame.
- **self**—Identifies one of the bridge ports.
- **management**—Indicates an entry that was entered into the database manually. The status field of all static entries in the Forwarding Table will display **management**.
- **invalid**—The entry is a learned entry that has aged out, but has not yet been flushed from the table.
- **other**—The bridge is unable to determine the entry's status.

The information displayed for the Static database is somewhat different; for each entry, the window displays the following:

Source Address

Displays the MAC addresses of devices that have transmitted frames to the bridge.

Receive Port

Displays the port on which a packet with the specified source address must be received in order for the filtering actions specified in the **Destination Port** field to take place. A setting of 0 will apply the filtering action anytime a packet with the specified source address is received by any of the bridge ports.

Destination Port

Displays the port or ports to which frames that have the specified source address and were received on the specified port or ports will be forwarded. Note that packets with the specified source address received on the specified port or ports will be blocked from any ports not listed in this field.

If the number of Destination Ports exceeds what the Destination Ports column is able to display, Destination Ports for that filter appear as a hex string that maps to actual port numbers.

For example, a Destination Port entry of B54180E0 represents ports 1, 3, 4, 6, 8, 10, 16, 17, 25, 26, and 27. Here's how to translate the hex string to port numbers:

1. Translate each hex integer into a four-digit binary value:

B	5	4	1	8	0	E	0
1011	0101	0100	0001	1000	0000	1110	0000

2. Each "1" in the binary bitmask represents a Destination Port number:

B	5	4	1	8	0	E	0
1011	0101	0100	0001	1000	0000	1110	0000
1,X,3,4	X,6,X,8	X,10,X,X	X,X,X,16	17,X,X,X	X,X,X,X	25,26,27,X	X,X,X,X

Status

Indicates the assigned permanence of the entry:

- **permanent**—The entry won't be aged out or deleted on reset.
- **deleteOnReset**—The entry will be deleted when the bridge is reset.
- **deleteOnTimeout**—The entry is subject to the ageing timer.

The buttons at the bottom of the window provide the following functions:

Delete

The **Delete** button is only available when the Filtering Database window is showing Static entries and one entry in the list is selected. Use the Delete button to remove an entry from the Static Table; see **Deleting a Static Table Entry**, page 6-19.

Change

The **Change** button is only available when the Filtering Database window is showing Static entries and one entry in the list is selected. Use the Change button to change the selected port's receive port/destination ports settings; see **Changing Forwarding and Static Database Entries**, page 6-18.

Add to Static Table

The **Add to Static Table** button is only available when the Filtering Database window is showing Forwarding entries and one entry in the list is selected. Use it to add a forwarding entry to the static database. Since the Forwarding table cannot be edited, you must add an entry to the Static Table in order to change or delete it, as desired.

Change Ageing Time

The Ageing Time determines how long a Forwarding entry (or a Static entry with deleteOnTimeout status) is retained before being discarded due to inactivity. Use the **Change Ageing Time** button to set a new Ageing Time; see the following section for details.

Find...

Use the **Find** button to search the Filtering Database for a specific MAC address; see **Finding a Filtering Database MAC Address**, page 6-20.

Update

The Filtering Database window shows a snapshot of the database. Clicking mouse button 1 on the **Update** button displays the current database.

Changing the Filtering Database Dynamic Ageing Time

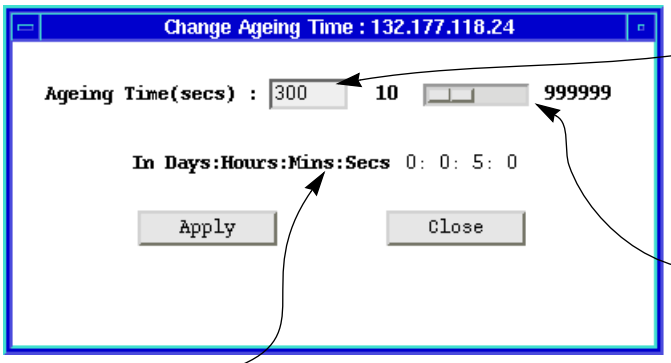
The Dynamic Ageing Time determines how long an entry remains in the Filtering Database before being purged due to inactivity. Purging older entries ensures that the Filtering Database is always using current information to make filter/forward decisions.

NOTE

During a topology change, the Forward Delay is used as the Filtering Database Ageing Time, which ensures that the Filtering Database will contain current topology information.

To change the Dynamic Ageing Time:

1. In the Filtering Database window, click mouse button 1 on the **Change Ageing Time** button to open the Change Ageing Time window.



As you change the ageing time, SPMA converts seconds to days:hours:minutes:seconds.

2. Highlight and edit the **Ageing Time** (in seconds), and then click mouse button 1 on the **Apply** button.

   or

   Use mouse button 1 to drag the slide bar, then click **Apply**.

   or

   Click mouse button 1 next to the slide to increment the time in 100 second jumps, then click **Apply**.

Figure 6-8. Changing the Filtering Database Ageing Time

Changing Forwarding and Static Database Entries

The only entries that can be changed or deleted in the Filtering Database are static entries. If the entry you wish to change or delete is a forwarding entry, you must add it to the Static Table. The Static Table (Figure 6-9) is used to change a forwarding entry to a static or permanent entry, or make changes to existing static entries. To open the Static Table window:

1. Open the Filtering Database window by clicking on the Front Panel Device button; drag down to **Filtering Database** to display the Filtering Database window.

2. If the Filtering Database window displays Forwarding entries, highlight the entry you want to change and click on the **Add to Static Table** button.

   or

   If the Filtering Database window displays Static entries, highlight an entry and click on the **Change** button.

NOTE

*It is also possible to open the Static Table in either case without highlighting an entry, by clicking on the **Add To Static Table** button. The static address field will appear blank. Enter the MAC address that you want to add to the Static Table.*

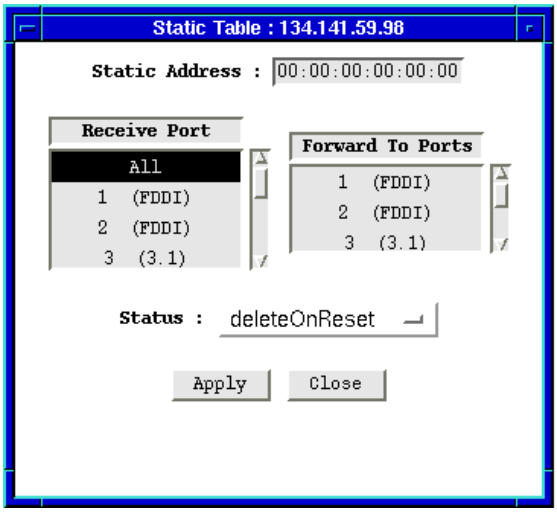


Figure 6-9. Static Table Window

Static Address

The **Static Address** field will display the MAC address of the entry you highlighted in the Filtering Database window. If no entry was selected, the address field will contain zeros, and a valid MAC address may be entered.

Receive Port

The **Receive Port** list box specifies the port on which packets from the specified static address must be received in order for the static database entry to apply. If **All** is selected, the entry will be applied to packets forwarded to any port.

Forward To Ports

The **Forward To Ports** list box specifies the ports to which packets with the specified source address received on the specified ports will be forwarded. The port or ports selected in this list will be displayed in the Filtering Database window as the **Destination Port**.

To change an entry:

1. Click mouse button 1 on the port in the **Receive Port** list box that you want to specify as the receive port for the entry in the **Static Address** field (remember that if **All** is selected, the entry will be applied to packets received on any port).
2. Click mouse button 1 on any port or ports in the **Forward To Ports** list that you want to be displayed in the Filtering Database window as the destination port.
3. Click mouse button 1 on the **Status** button and choose one of the following:

   permanent—The entry won't be aged out or deleted on reset.

   deleteOnReset—The entry will deleted when the bridge is reset.

   deleteOnTimeout—The entry is subject to the ageing timer.
4. After you set the entry's status, click mouse button 1 on the **Apply** button.

Deleting a Static Table Entry

To delete a Static Table entry:

1. In the Filtering Database window, click mouse button 1 in the appropriate selection box to display the Static database.
2. Select the entry you want to delete by clicking it with mouse button 1.
3. Click on the **Delete** button.

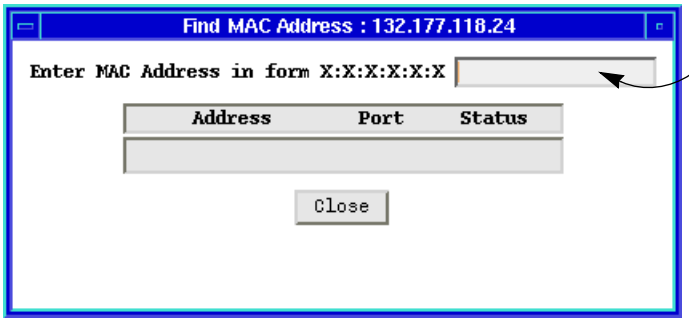
Finding a Filtering Database MAC Address

To find a source address in the Filtering Database:

1. In the Filtering Database window, click on the Find... button to open the Find MAC Address window.

   or

   In the Bridge Traffic View, display the Device menu by clicking on the Front Panel Device button. Drag down to **Find MAC Address**.



2. In the edit box, enter a valid MAC address and then press the Return key. If the address is found in the Filtering Database, its port location and status will appear in the list box. If it is not found, a separate window will appear with a “Not Found” message.

Figure 6-10. Find MAC Address Window

The Spanning Tree Protocol Window

Bridges in a network collectively implement a Spanning Tree Algorithm (STA) to detect and eliminate data loops in a network containing parallel bridges.

In a network designed with multiple bridges placed in parallel (i.e., attached to the same network segment), Spanning Tree selects a controlling Root Bridge and Port for the entire bridged local area network, and a Designated Bridge and Port for each individual network segment. The Root bridge is the one that selects one of two or more available bridge paths between two end stations, basing its decision on factors associated with each of the bridges in the path. A Designated Port/Bridge for a network segment relays frames toward the Root Bridge, or from the Root Bridge onto the network segment. When data passes from one end station to another across a bridged local area network, it is forwarded through the Designated Bridge/Port for each network segment towards the Root Bridge, which in turn forwards frames towards Designated Bridges/Ports on its opposite side.

During the Root Bridge selection process, all bridges on the network communicate STA information via Bridge Protocol Data Units (BPDUs). It is with BPDUs that the bridges collectively determine the current network topology and ensure that all bridges have current topology information.

The Spanning Tree Protocol window displays information used by the network bridges to select the Root Bridge and parameters that affect the bridge's participation in Spanning Tree operations.

To open the Spanning Tree Protocol window:

1. Click on the Front Panel Device button.
2. Drag down to **Spanning Tree** and release.

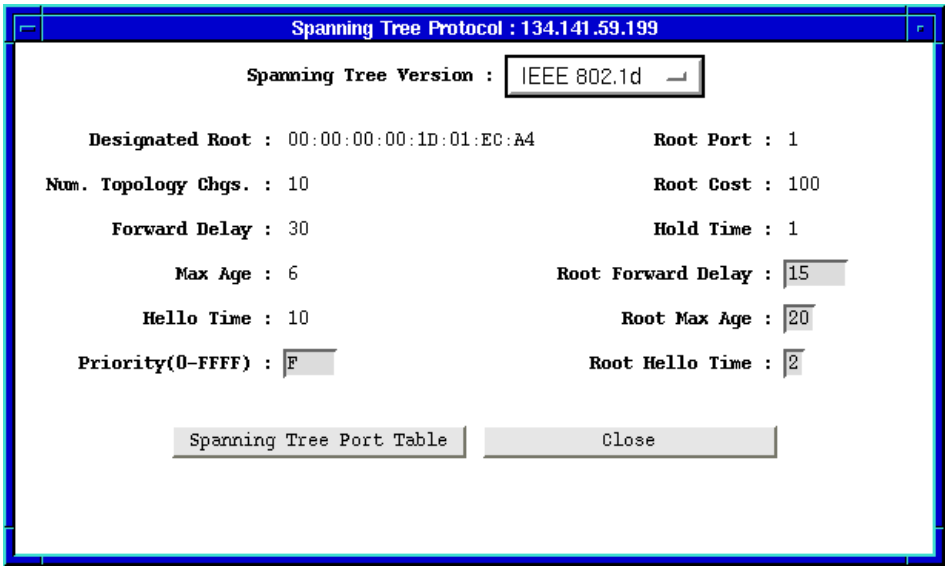


Figure 6-11. Spanning Tree Protocol Window

The Spanning Tree Protocol window displays the following information:

Spanning Tree Version

The version shows the Spanning Tree Protocol type employed by this bridge:

- IEEE 802.1d
- DEC LAN 100
- None

You must use either 802.1d or DEC to interconnect all bridges in a network using parallel bridges. By default, a Cabletron bridge turns on the 802.1d Spanning Tree. All of Cabletron's bridge products have the ability to use either the 802.1d or DEC Spanning Tree version, or they can be set so that no version is in effect. (A bridge should be set to None if there are no redundant loops incorporated within the network.)

All bridges in a network must use the same Spanning Tree version. Mixing Spanning Tree Algorithm protocols will cause an unstable network.

Designated Root

This value represents the bridge that is the current Root Bridge as determined by the STA. The Designated Root value consists of the configurable portion of the bridge ID (i.e., the first two octets of the eight-octet-long bridge ID) and the root bridge device's MAC address (the last six octets of the bridge ID). This value is used as the Root Identifier parameter in all configuration BPDUs originated from this node.

Num. Topology Chgs.

Indicates the number of times the bridge's Topology Change flag has been changed since the bridge was powered up or initialized. The Topology Change flag increments each time any of the network's bridges enters or leaves the network or when the Root Bridge ID changes.

The values for the following three fields—Forward Delay, Max Age, and Hello Time—represent the values that are currently being used by all bridges, as dictated by the Root bridge. In the Spanning Tree Protocol window, you can view and set the values—Root Forward Delay, Root Max Age, Root Hello Time—that will be in effect when the bridge for which you are setting the parameters becomes the Root Bridge.

Forward Delay

The length of time, in seconds, that controls how long a bridge port remains in each state (Forwarding, Learning, Listening, etc.) when moving toward the Forwarding state. During a topology change, the Forward Delay is also used as the Filtering Database Ageing Time, which ensures that the Filtering Database will contain current topology information. The Root Bridge sets the Forward Delay.

Max Age

The current setting for the bridge's BPDU ageing timer, in seconds. The ageing timer defines the maximum number of seconds that a Configuration BPDU is retained by the bridge before it is discarded. During normal operation, each bridge in the network receives a new Configuration BPDU before the ageing timer expires. If the timer expires before a new Configuration BPDU is received, it indicates that the former Root is no longer active. The remaining bridges begin Spanning Tree operation to select a new Root. The Root Bridge determines the Max Age. The range for this field is from 6 to 40 seconds, with a default value of 20 seconds.

Hello Time

Indicates, in seconds, the length of time the Root Bridge, or bridge attempting to become the Root, waits before resending a Configuration BPDU. The Root Bridge determines the Hello Time.

Priority

The Spanning Tree Algorithm assigns each bridge a unique identifier, which is derived from the individual port's MAC address and its priority as determined by the Spanning Tree Algorithm or your setting. The bridge with the lowest value of bridge identifier is selected as the Root. A lower priority number indicates a higher priority; a higher priority enhances a bridge's chance of being selected as the Root.

Acceptable values range from 0-FFFF and can be edited to change the network topology, if needed. The default is 8000.

Root Port

The port identifier (i.e., the physical index number) for the port that provides the lowest cost path to the Root Bridge. The Root Port field displays 0 if this bridging device is the Root Bridge.

Root Cost

Indicates the cost of the data path from this bridge to the Root Bridge. Each port on each bridge adds a "cost" to a particular path that a frame must travel. For example, if each port in a particular path has a Path Cost of 1, the Root Cost would be a count of the number of bridges along the path. This field will read 0 if an interface on the 7C0x SmartSwitch is the Root Bridge. See **Changing a Port's STA Parameters**, page 6-27, to find out how to set a port's Path Cost.

Hold Time

The minimum time, in seconds, that can elapse between the transmission of Configuration BPDUs. The Hold Time ensures that Configuration BPDUs are not transmitted too frequently through any bridge port. Receipt of a Configuration BPDU starts the Hold Time count at a device. If the Hold Time expires, the port invokes the Transmit Configuration BPDU procedure, which sends configuration change information to the Root. The Hold Time is a fixed value, as specified by the IEEE 802.1d specification.

NOTE

The values for the Forward Delay, Max Age, Hold Time, and Hello Time fields are stored within the MIB in units of hundredths of a second rather than seconds; your Cabletron management application converts hundredths of a second to seconds for display purposes. You can use any SNMP Set Request tool to edit the values for these three fields; just remember that you must enter your values in hundredths of seconds, rather than in seconds.

Root Forward Delay

The Forward Delay (in seconds) that will be implemented by this bridge if it is the Root or becomes the Root. (The Root Bridge in the network sets the Forward Delay for all bridges in the Spanning Tree network.)

The IEEE 802.1d specification recommends that Forward Delay = 15 seconds, with an allowable range of 4 to 30 seconds.

TIP

To ensure proper operation of the Spanning Tree Algorithm, the IEEE 802.1d specification recommends that you always observe the following relationship between Forward Delay and Max Age:

$$2 \times (\text{Forward Delay} - 1.0) \geq \text{Max Age}$$

Root Max Age

The Max Age value (in seconds) that will be implemented if this bridge is the Root or becomes the Root. (The Root Bridge in the network sets the Max Age for all bridges in the Spanning Tree network.)

The IEEE 802.1d specification recommends that Max Age = 20 seconds, with an allowable range of 6 to 40 seconds.

Root Hello Time

The Hello Time that will be implemented if this bridge is the Root or becomes the Root.

The IEEE 802.1d specification recommends that Hello Time = 2 seconds, with an allowable range of 1 to 10 seconds.

Spanning Tree Port Table

The **Spanning Tree Port Table** button opens the window in which you set Spanning Tree parameters for individual bridge ports; see **The Spanning Tree Port Parameters Window**, page 6-25, for more information.

Changing Spanning Tree Parameters

To change the Bridge Priority, Root Forward Delay, Root Max Age, or Root Hello Time:

1. In the Spanning Tree Protocol window, highlight the current value of the field you want to change.
2. Type the new value in the appropriate text box and press **Enter** or **Return** on the keyboard.

The Spanning Tree Port Parameters Window

The Spanning Tree Algorithm ensures that only a single bridge path exists between any two end stations in a network designed with multiple bridges placed in parallel; it also ensures that on any given bridge, only one port path exists between the bridge and any one network segment. In the Spanning Tree Port Table you can view and edit the Spanning Tree values for individual ports; the Spanning Tree Port parameters affect a port's participation in the Spanning Tree.

NOTE

Setting Spanning Tree Port Parameters only affects port selection on a particular bridge; settings do not affect the 7C0x SmartSwitch's device-level priority in the network's Spanning Tree.

To open the Spanning Tree Port Table window:

1. Display the Device menu by clicking on the Front Panel Device button.
2. Drag down to **Spanning Tree** to open the Spanning Tree Protocol window.
3. In the Spanning Tree Protocol window, click on the **Spanning Tree Port Table** button.

   or

1. In the Bridge Traffic View, click mouse button 3 on a port to display the Port menu and drag down to **Spanning Tree**.

The scroll list at the top of the window lists each bridge port available on the device and its current port priority. Below the Port List, the window includes the following:

Priority (Port)

If two or more ports on the same bridge are connected to the same network segment, each port will receive the same device-level values for Root ID, Root Cost, and Bridge ID in Configuration BPDUs. In this case, the BPDU's port-level information—the transmitting port's identifier and its manageable Priority component— is used to determine which port on this bridge will be the Designated Port for that segment. A lower number indicates a higher priority; the default is 80. The allowable range is 0 to FF.

Path Cost

The portion of the total path cost associated with this port. Lowering a port's Path Cost makes a port more competitive in the selection of the Designated Port. The default value is 100 for Cabletron bridges. The allowable range is from 1 to 65535.

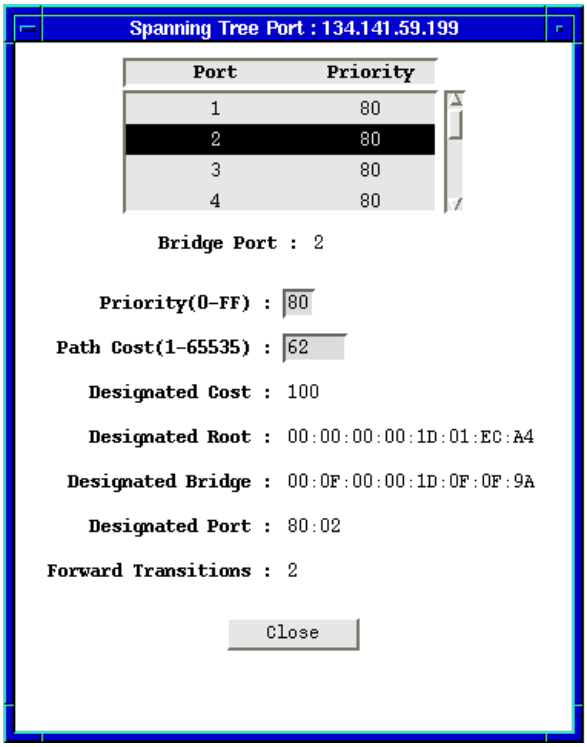


Figure 6-12. Spanning Tree Port Parameters Window

Designated Cost

The cost of the path from this port to the Root Bridge on the network. If the highlighted port is the Root Port, the Designated Cost is 0. If this bridge is the Root Bridge, all its bridge ports have a Designated Cost of 0. This value is compared to the Root Path Cost field in received configuration BPDUs.

Designated Root

The unique Bridge Identifier of the bridge that is assumed to be the Root Bridge on the network; this information is contained in the Configuration BPDUs.

Designated Bridge

Displays the MAC address and priority component of the Bridge ID for the bridge that is believed to be the Designated Bridge for the network segment associated with this port.

The Designated Bridge ID, along with the Designated Port and Port Identifier parameters for the port, is used to determine whether this port should be the Designated Port for the network segment to which it is attached.

Designated Port
The Port ID of the port on the Designated Bridge for this port's segment. The Designated Port is the bridge port that offers the lowest path cost to the Root Bridge.

Forward Transitions
The number of times this port has moved from the Learning state to the Forwarding state since the device was started or since it was last reset.

Changing a Port's STA Parameters

To change a port's Priority or Path Cost:

1. In the scroll list, click mouse button 1 on the port you want to change (use the scroll bar if necessary to display the desired port). You can only select one port at a time. The highlighted port's Spanning Tree parameters appear in the boxes below the list.
2. Highlight and edit the **Priority** and **Path Cost** boxes as required. After you type in the new value in a box, press **Enter** or **Return** on the keyboard.

Creating Bridge Traffic Charts, Graphs, and Meters

The Bridge application uses the SPMA Charts, Graphs and Meters tools to depict bridge statistics describing activity at the bridge-port level. Once running, however, a pie chart, graph or meter is independent from the application where it was started. Although the windows you open to create pie charts, graphs and meters have unique variable lists, the procedures for creating a pie chart, a graph or a meter are the same.

To access the Pie Chart, Graph, and Meters tools from the Bridge Traffic View Port menus:

1. Click mouse button 3 on a Bridge Port box to display the Bridge Port menu.
2. Drag down to select **Pie Chart** or **Graphs/Meters**—>**Transparent**.

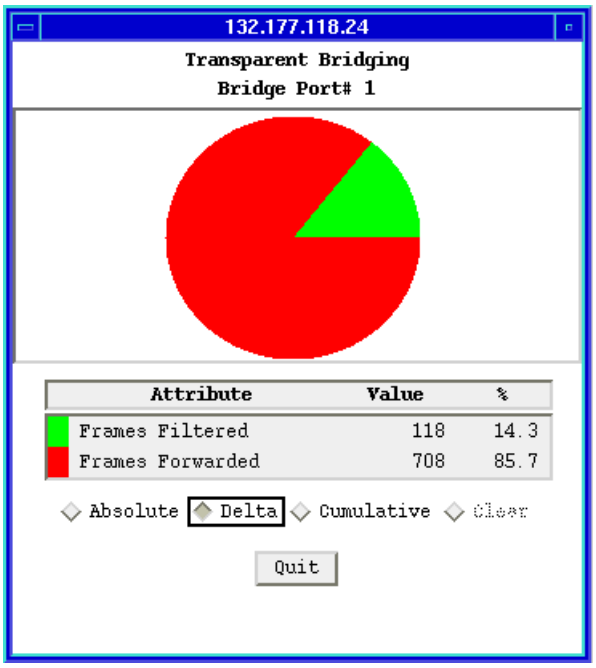


Figure 6-13. Pie Chart Window

For complete descriptions of chart, graph, and meter variables and details on how to create and control a pie chart, graph or meter, see the chapter on charts, graphs and meters in the ***SPMA Tools Guide.***

NOTE

Graphing capabilities are provided by an application that is included in HP Network Node Manager and IBM NetView; therefore, graphs are only available when SPMA is run in conjunction with one of these network management platforms. If you are running SPMA in a stand-alone mode or in conjunction with SunNet Manager, no graphing capabilities are available and no graph-related options will be displayed on buttons or menus. Note that the screens displayed in this guide will include the graph-related options where they are available; please disregard these references if they do not apply.

The Bridge Port Forwarding Statistics Window

The Bridge Port Forwarding Statistics window displays a breakdown of activity between the selected port and each of the other bridge ports.

To view statistics for a particular bridge port:

1. In the Bridge Traffic View, click mouse button 3 on a bridge port to display the Port menu.
2. Drag down to **Forwarding Statistics** —>**Transparent** and release to open the Statistics window.

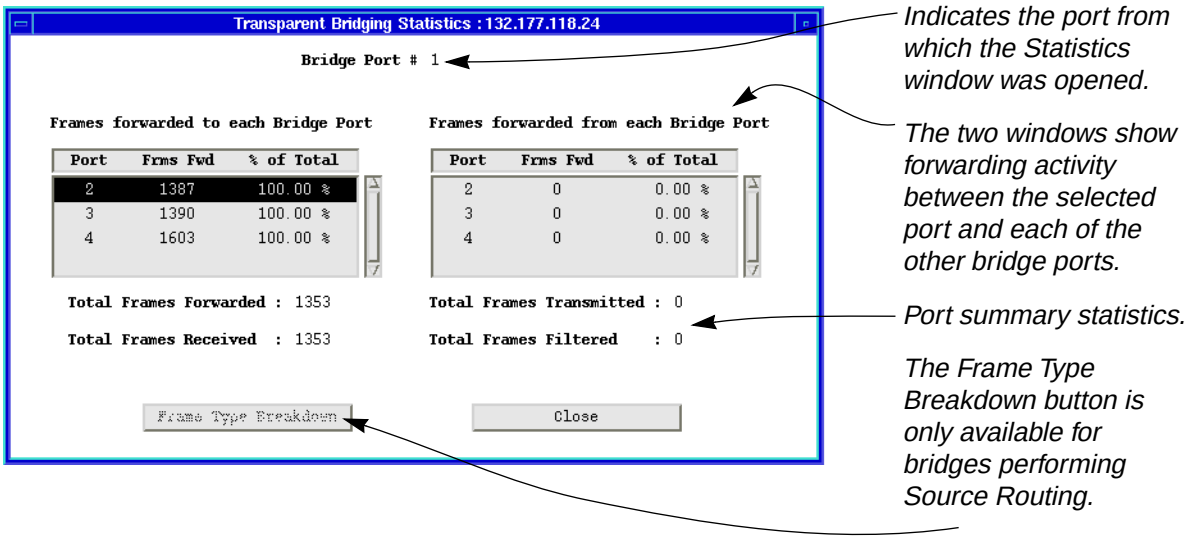


Figure 6-14. Bridge Port Forwarding Statistics Window

Port Forwarding Statistics Window Fields

The Bridge Port Statistics window contains two list boxes detailing port forwarding activity to and from the currently selected port:

- The leftmost list box shows frames forwarded to each of the other bridge ports from the currently selected port.
- The rightmost list box shows frames forwarded to the currently selected port from each of the other bridge ports.

The list box detail fields are:

Port

The port number to/from which frames are being forwarded.

Frms Fwd

The total number of frames forwarded to/from the selected port to/from the other bridge ports during the last polling interval.

% of Total

In the **Frames forwarded to each Bridge Port** list box, this is the percentage of all frames forwarded to the selected port that were then forwarded to other bridge ports during the last polling interval. In the **Frames forwarded from each Bridge Port** list box, this is the percentage of all frames received by the selected bridge port that were forwarded to that port by other bridge ports.

The four statistics shown beneath the list boxes are the port summary statistics, which consist of:

Total Frames Forwarded
The total number of frames forwarded through the bridge to another segment.

Total Frames Received
The number of frames, of all types, received at the port.

Total Frames Transmitted
The number of Bridge Protocol Data Units (BPDUs) transmitted by the bridge.

Total Frames Filtered
The total number of frames not forwarded through the bridge.

NOTE

The statistics shown in the Bridge Port Statistics window reflect a "snapshot" of the statistics from the time the window was opened. To refresh the statistics, you must close this window and open it again.

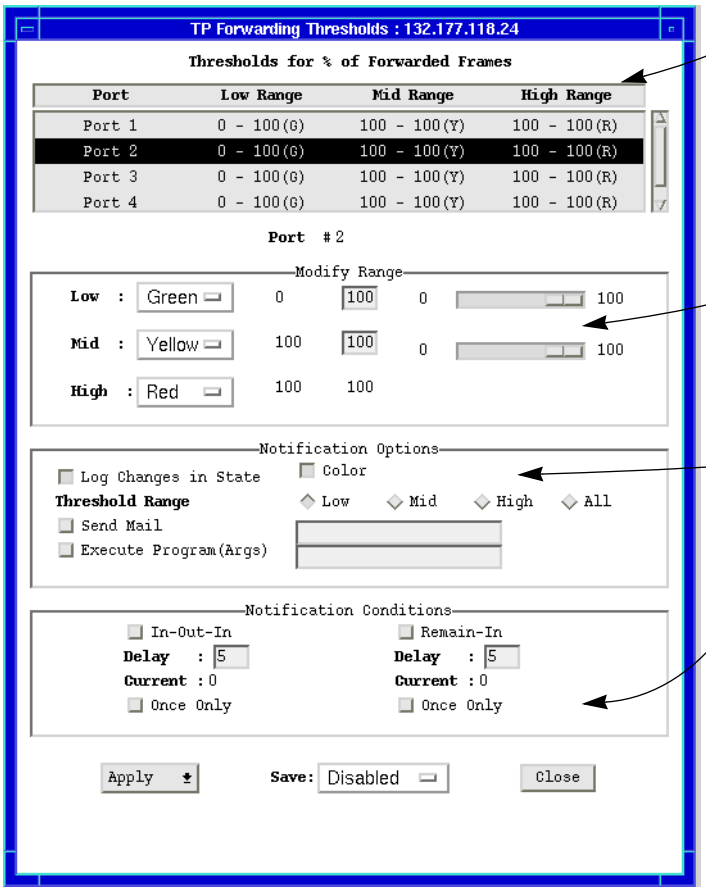
Configuring Forwarding Thresholds

You can define notification thresholds for bridge port forwarding levels and then have SPMA use those thresholds to do one or more of the following:

- Color code the Bridge Port display boxes
- Send Internet mail to a registered user
- Launch a program on your management workstation

To open the Forwarding Thresholds window:

1. Click button 3 anywhere within a Bridge Port display box in the Bridge View to display the Port menu.
2. In the Port menu, click button 3 on **Forwarding Thresholds** —>**Transparent** to open the Forwarding Thresholds window.



A traffic level is the specified value of forwarded frames as a percentage of total received frames.

You can specify traffic levels that define the boundary between the low and medium ranges and between the medium and high ranges.

When SPMA polls the device and detects that the percentage of forwarded frames has moved into a new range, heading either up or down, the notification options and conditions in use for that port take place.

Figure 6-15. Port Forwarding Thresholds Window

NOTE

SPMA polls a bridge at preset intervals, as defined in the Polling Intervals window accessed from the Bridge View Device menu. A port's traffic level can pass from one range to the next and then back to the original level between polls from SPMA. When this occurs, SPMA won't record that the threshold has been passed because the event was never observed.

To set bridge port thresholds, notification options, and notification conditions:

1. In the Forwarding Thresholds window, highlight the port where you want to set thresholds. You can select multiple ports by clicking button 1 on each one. To deselect a port, click it again. To apply the settings to all bridge ports, you can use the options provided at the bottom of the screen rather than selecting all ports in the scroll list.

2. In the Modify Range section of the Forwarding Thresholds window, you can edit the line that displays the high end of the Low and Mid ranges, or you can use the slide bars to specify the thresholds. You can also assign a color to each of the three ranges. The Bridge Port boxes on the Bridge Traffic View will be colored according to the settings made here (i.e., if you assign the color red to the High traffic range, then a Bridge Port box will be colored red when its traffic range is High). To set the high end of the Low and Mid ranges, and assign color codes to all three ranges:

   a. Change the upper limit of the Low and Mid traffic ranges by highlighting the value, typing the new value, and pressing **Enter** or **Return**. You may also change the value by moving the slide bar next to the value you wish to change until the desired range is reached.

   b. By default, bridge ports are color coded in the Bridge Traffic View according to their traffic level: Low range is green; Mid range is yellow; High range is red. To assign color codes to the three traffic ranges, click on the **Low**, **Mid**, or **High** buttons to the left of the range fields, drag to highlight the desired color, and release. The selected color will be displayed on the button, and will be used in the Bridge Port boxes when the color's corresponding range is reached.

3. In the Notification Options section, you can enable/disable threshold event logging, enable/disable the Bridge Port box colors, and assign threshold events (send mail or execute a program) to the different (or to all) threshold ranges. To do so:

   a. To disable threshold event logging, deselect the **Log Changes in State** checkbox. By default, all threshold events are logged. For more information about the Forwarding Log, see **Viewing the Forwarding Log** on page 6-33.

   b. To enable/disable the colors, click button 1 on the **Color** box. When colors are disabled, the Bridge Port box colors in the Bridge Traffic View remain as they were when the colors were last enabled.

   c. To send mail or execute a program when a threshold range is reached, first click the **Threshold Range** button to which you want to apply the threshold event. To send mail for a threshold event, select the **Send Mail** box and enter the name of a registered mail user. To have a threshold event launch a program, select the **Execute Program (Args)** box and enter the name of an executable file, including required arguments.

4. Notification Conditions make your Notification Options subject to defined conditions:

   a. If you check the **In—Out—In** box, notification takes place when the threshold passes from one range to another and then back. The number in the **Delay** box specifies the number of times this transition is to take place before notification is launched. The **Current** box counts down the transitions.

   b. If you select the **Remain—In** box, notification takes place when the threshold passes from one range to another, and stays in that range for the number of polling cycles specified in the **Delay** box.

   c. If you check the **Once Only** box, notification only takes place the first time the **Delay** count is reached.

5. The **Save** option gives you three choices as to how the options and conditions you have selected will be saved.

   a. If you choose **Disabled**, none of the options and conditions you have chosen will be saved to the bridge database.

   b. If you select **As Defaul**t, the chosen options and conditions will be saved as default values. The saved information will be used for any IP not having an entry in the bridge database.

   c. If you select **By IP**, the options and conditions chosen for that IP will be saved to the bridge database, and the next time the application is run for this device the saved values will be used.

6. When you're finished setting thresholds and notification options, click button 3 on the **Apply** button and choose either **Selected Only** or **All**. **Selected Only** applies the selected Forwarding Thresholds settings to the ports that are highlighted in the scroll list near the top of the Forwarding Thresholds window.

Viewing the Forwarding Log

The Forwarding Log records an entry each time a bridge port's traffic passes a preset traffic threshold. By default, logging is enabled for all bridge ports.

To open the Forwarding Log window:

1. In the Bridge Traffic View, click mouse button 3 in one of the bridge ports to display the Port menu.

2. In the Port menu, click button 3 on **Forwarding Log** and then drag right to **Transparent**.

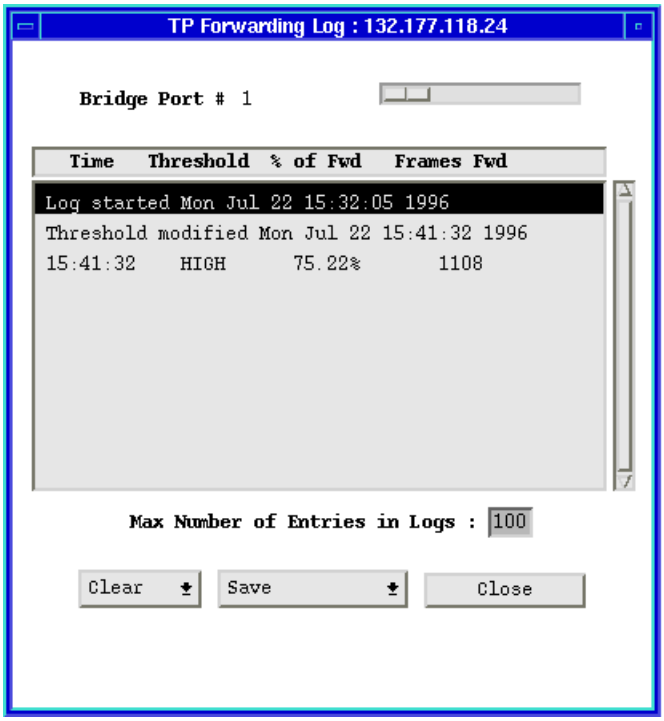


Figure 6-16. Sample Forwarding Log Window

To select a different Bridge Port log:

1. Use the slide bar at the top of the Forwarding Log window to select a different port.

To clear all logs or just the current log:

1. Click on the **Clear** button and then select the appropriate choice, either **Current Log** or **All Logs**.

To change the number of entries retained by the log:

1. Highlight the **Max Number** line, type a new number and press Return on the keyboard.

NOTE

Log entries are stored in the SPMA software. When the maximum number of entries is reached, the entries get aged out as necessary, starting with the oldest entry first.

To save log files:

1. Click on the **Save** button and select either **Current Log** or **All Logs** to open the Save Log window.
2. In the Save Log window, enter a file name for the file to be saved and then click on the **OK** button. The default directory for saved log files is the current directory. To specify a different directory, include the path name with the log file name.

To disable the Forwarding Log of all bridge ports or individual bridge ports:

1. Click button 3 on the appropriate Bridge Port box to display the Port menu.
2. In the Port menu, click button 3 on **Forwarding Thresholds** and then drag right to **Transparent**.
3. In the Forwarding Thresholds window, deselect the **Log Changes in State** box.
4. Click on the **Apply** button and then click on either **Selected Only** or **All**.

Changing Polling Intervals

Much of the information displayed in the Bridge Traffic View is gathered periodically rather than continuously. You can edit the times between these periodic polls.

To edit the polling times:

1. Display the Device menu by clicking on the Front Panel Device button.
2. Drag down to **Polling Intervals** and release. The Polling Intervals window displays.

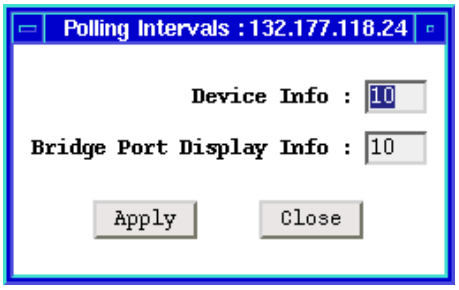


Figure 6-17. The Polling Intervals Window

3. Highlight and edit the **Device Info** and **Bridge Port Display Info** boxes and then click on the **Apply** button to save changes.

You can change values for the following polling interval fields:

Device Info
Specifies the time, in seconds, that SPMA waits before updating the Front Panel information (Uptime, Location, and so forth) in the Bridge Traffic View.

Bridge Port Display Info
Specifies the time, in seconds, that SPMA waits before updating statistical and status information in the Bridge Traffic View port display boxes.

Enabling and Disabling Ports

When you disable a bridge port, you disconnect that port's network from the bridge entirely. Nodes connected to the network can still communicate with each other, but they can't communicate with the bridge and other networks connected to the bridge.

In Transparent bridges, the disabled port does not forward any packets, nor does it participate in Spanning Tree operations. When you enable a port on a Transparent bridge, the port moves from the Disabled state through the Blocking, Learning, and Listening states to the Forwarding state.

NOTE

Enabling and disabling a port changes its Port Status, not its Port State. An enabled port is able to participate in bridging and Spanning Tree operations. A disabled port on a Transparent bridge does not participate in bridging or Spanning Tree operations.

Enabling and Disabling a Transparent Bridge Port

To enable or disable a Transparent bridge port:

1. In the Bridge Traffic View, display the Port menu by clicking mouse button 3 in a Bridge Port box. Select the port that connects to the network that you want to enable or disable.
2. In the Port menu, click button 3 on **Enable** or **Disable**, drag right to **Transparent**, and release.

When you disable a Transparent bridge port, the port's display box turns blue. When you enable a Transparent bridge port, the port's color changes to indicate the forwarding threshold range. (Port color codes are only active if the Color box is selected in the Forwarding Thresholds window. Color codes are on by default.)

Appendix A

7C0x SmartSwitch MIB Structure

7C0x SmartSwitch management information base configuration

IETF MIB Support

In addition to its proprietary features, the 7C0x SmartSwitch currently supports the following IETF MIBs:

- RFC 1213 MIB for Network Management of TCP/IP-based Internets: MIB-II
- RFC 1493 Definitions of Managed Objects for Bridges
- RFC 1512 FDDI Management Information Base
- RFC 1757 Remote Network Monitoring MIB

7C0x SmartSwitch MIB Structure

Cabletron's newer intelligent devices — like the 7C0x SmartSwitch — organize MIB data into a series of "components." A MIB component is a logical grouping of MIB data, and each group controls a defined set of objects. For example, 7C0x bridging information is organized into its own component, and SecureFast switching resides in a separate component; RMON functionality is contained within its own component; and an ATM component will be instantiated whenever a 7A06-01 NIM is installed in the SmartSwitch chassis.

The 7C0x SmartSwitch MIB consists of up to nine components, each of which is described below. Note, however, that at any given time, the MIB component list displayed by your 7C0x may not include some of the components described below, since the SmartSwitch has the ability to alter the components which make up its MIB in response to changes in the chassis. For example, if no FDDI or ATM NIMs are installed, the related MIB components will not appear in the list; similarly, either the bridge or the switch component will be instantiated,

depending on which functionality the device has been configured to use. To see which MIB components are currently being used in your 7C0x SmartSwitch, bring up the Community Names application, or use any SNMP Get operation that will allow you to view the contents of the contLogicalEntryTable.

The 7C0x SmartSwitch MIB consists of the following components:

Chassis MGR

The Chassis MGR MIB component contains most of the basic information about the 7X00 SmartSwitch Controller module, the chassis it is controlling, and the other modules installed in that chassis, including: chassis type, backplane type, number of slots, which module types and names are installed in which slots, the 7C0x's MIB component information (in the contLogicalEntryTable), device and module names, hardware revision numbers, MAC and IP addresses, the current time and date, and information related to connected uninterruptable power supplies and TFTP download. The system, interfaces, at, ip, icmp, udp, and snmp groups from MIB-II and the objects that provide Local Management functionality are also included. The community names assigned to this MIB component provide the gateway that all SPMA applications use to access all information in the other components, even if those components have different community names; the Chassis MGR community names are the same as those assigned via Local Management.

CTATM_MIB

The ATM_MIB component contains the objects that provide the ATM NIM's uplink port with its network functionality.

Transparent Bridge

The Transparent Bridge MIB component — instantiated only when the 7C0x has been configured (currently via Local Management) to operate in traditional bridging mode — controls all of the 7C0x's transparent bridging functions, including bridge port description and status, bridging statistics (frames forwarded, frames blocked, etc.), and bridge configuration information.

NOTE

Since there are currently no Token Ring NIMs available for the 7C0x SmartSwitch chassis, no source route bridging functions are supported at this time.

IP Services

Like the Host Services MIB component, the IP Services MIB component contains some objects related to basic IP functionality.

RMON Default

The RMON, or Remote Network Monitoring, Default MIB component contains the statistics, history, alarm, and event groups from the RMON MIB (RFC 1757). This component is shipped in an inactive state, and can be activated and deactivated as necessary.

Host Services

The Host Services MIB component contains the objects that provide the 7C0x with its IP functionality — essentially, those functions which allow the 7C0x to operate over a network — including functions such as ping, Telnet, and TFTP.

MIB Navigator

The MIB Navigator component provides a command set from which you can configure and manage your 7C0x SmartSwitch by telnetting directly into the device and viewing and modifying the objects in the device's MIB. The MIB Navigator is accessible through SPMA via the Telnet application; see the ***SPMA Tools Guide*** and/or your 7C0x hardware manual for more information.

FDDI SMT

The FDDI SMT (Station ManagemenT) MIB component contains the objects that allow the FDDI NIM ports to function as stations on the FDDI ring, including information regarding connection policy, configuration, T-Req and T-Neg values, the TVX timer value, duplicate address testing, frame status, version IDs, and upstream neighbor addresses.

SWITCH Services

The SWITCH Services MIB component — instantiated only when the 7C0x has been configured (currently via Local Management) to operate in SecureFast switching mode — provides the objects necessary for SecureFast switching operation, including administrative and operational status, port types, switch capacity, connection table data, a variety of switching-related statistics, and switch configuration parameters.

A Brief Word About MIB Components and Community Names

In the *original* version of the component MIB architecture, each MIB component is protected by its own set of user-configurable Read-Only, Read/Write, and Super-User community names. These names determine the level of access that will be granted to the information controlled by each individual component. For these devices, the central point of access for remote management is provided by the Chassis MGR MIB component — that is, if you define your device icon or launch a management application using the read-only, read/write, or super-user community name assigned to the Chassis MGR MIB component, your SPMA application is granted the appropriate level of access (read-only, read/write, or super-user) to all of that device's MIB information — even if the other MIB components have different community names (as may occur if multiple instances of the same component are required).

Newer versions of devices with this component-based MIB architecture — like the 7C0x SmartSwitch — have been simplified somewhat; these devices support a single, *global* set of community names, with small modifications added automatically to accommodate multiple instances of the same MIB component (where necessary). Again, defining your device icon or launching a management application with one of these global community names gives SPMA access to all MIB information.

Where community names may become an issue, however, is when you are using the MIBTree or any similar MIB-based tool (such as those provided by SunNet Manager or HP Network Node Manager) to access MIB information. For these kinds of tools, you must supply the *precise* community name assigned to the component that contains the information you want. For devices which support the new global community names — like the 7C0x SmartSwitch — this only means that you must make note of the automatic modifications that are made for multiple instances of the same component, and use those specific community names when trying to access information stored in those components.

The MIB component descriptions provided above will serve as a roadmap for determining where the information you're interested in is located; you can use the SPMA Community Names tool (described in **Chapter 3** of the ***SPMA Tools Guide***) to both view and set the community names which apply to your device.

Index

Numerics

7C0x MIB components A-2
7C0x SmartSwitch family 1-1
    7C03 MMAC SmartSwitch 1-1
    7C04 Workgroup SmartSwitch 1-1
    7C04-R Workgroup SmartSwitch 1-1
    NIM modules 1-1
7C0x SmartSwitch firmware versions 1-8

A

AAL Type 5-3
Add to Static Table button 6-18
Admin button 6-6
Admin status
    Bridge 2-13
    FDDI 2-8
    Switch 2-11
Ageing Time 6-14, 6-17
Alarm Configuration (FDDI) 2-27
alarm log 3-4
alarm parameters (default) 3-9
alarmSampleType 3-11
ATM 5-1
ATM Adaptation Layer 5-3
ATM_MIB A-2
atmcfg 5-1
auto-negotiation 2-30
Average Packet Size 2-19

B

balarm 3-2
Base MAC Address 2-21
Boot Version 2-21
BPDU ageing timer 6-22
bridge 6-2
Bridge display mode 2-6
bridge port Color codes 6-6, 6-32
Bridge Port Display Info 6-36
Bridge Port Number 2-14
bridge port state 6-7
    blocking 6-7
    broken 6-8
    disabled 6-7
    forwarding 6-8
    learning 6-8
    listening 6-7
bridge port status 6-7
    disabled 6-7
    enabled 6-7
bridge port Traffic levels 6-31
Bridge Protocol Data Units (BPDUs) 6-2, 6-20
Bridge Statistics window 6-11
Bridge Status window
    setting and changing information 6-11
Bridge Traffic View buttons 6-6
Bridge View
    access levels 6-2
    changing front panel information 6-11
    launching 6-2
bridging (traditional) 2-13
bridging type 6-12
    transparent-only 6-12
    unknown 6-12
Broadcast/Multicast 3-3

C

Canonical (FDDI) address mode 4-25
Capability 2-17
change the Dynamic Ageing Time 6-17
channel trunking 5-3
Charts, Graphs, and Meters 1-4, 4-5, 4-17
Chassis MGR A-2
clear network logs 6-34
Collisions 2-19
COM port administrative display 2-8
community names 1-4, 2-1, 2-26, 3-2, 4-2, 4-9, 4-13, 4-21, 4-24, 5-2, A-3
component-based MIB architecture A-3
Configuration BPDU 6-22, 6-23
configuring an alarm 3-7
Connection 4-4

connection rules 4-22
Contact Status 2-3, 6-4
contLogicalEntryTable 3-2
CRC/Alignment errors 2-19
Current box 6-33

D

decLb100 6-21
Delay box 6-33
DelayExceedDiscard 6-12
deleteOnReset entry status 6-16, 6-19
deleteOnTimeout entry status 6-16, 6-19
Delta button 6-7, 6-8
delta values 3-5, 3-8
Designated Bridge 6-20, 6-26
Designated Cost 6-26
Designated Port 6-20, 6-27
Designated Root 6-22, 6-26
Destination Ports 6-16
Detail View 6-8
    Change Menu 6-10
    port summary information 6-10
Device button
    bridge 6-5
Device Configuration 2-4
Device Info 6-36
Device Location 2-3, 6-4
Device menu 2-4
    bridge 6-5
Device Name 2-3, 6-4
disable a bridge network 6-36
disable the Forwarding Log 6-35
disabling an alarm 3-9
Discard 2-18
Display Mode 2-5
double-wide NIM modules 2-4
dual-homing 4-22
Duplex Mode 2-16, 2-30
Dynamic Ageing Time 6-13, 6-17

E

Enabling or Disabling FDDI Ports 4-5
Encapsulation Type 5-4
Errors
    Ethernet (RMON) 2-19
    MIB II 2-18
Execute Program 6-32

F

falling action 3-5, 3-8
falling alarm threshold 3-1
falling threshold 3-5, 3-7, 3-8
FDDI connection rules 4-22
FDDI Front Panel Status 2-5
FDDI MAC Chart Window 4-18
FDDI SMT A-3
fddialrm 4-9
fddicnfg 4-13
fddicpol 4-21
fddiptcf 4-2
fddislst 4-24
Filtering Database 6-2
    accessing 6-14
fInNUcast 3-4
firmware version 1-8, 2-21
    bridge 6-5
Forward 6-7
Forward Delay 6-7, 6-17, 6-22
Forward Transitions 6-27
forwarding entry 6-13
Forwarding Log 6-33
Forwarding state 6-13
Forwarding Threshold Log window
    accessing 6-33
Forwarding Thresholds window
    accessing 6-30
fps 2-1
Fragments 2-19
Frame Sizes 2-19
Frames button 6-6
Frms In 6-7
Frms Out 6-7
Front Panel 6-3

G

Getting Help 1-8
global community names A-4
Global Find MAC Address tool 1-4, 2-4, 2-26
grouping of virtual connections 5-3

H

Hello Time 6-23
Help 1-8
History button 1-6
Hold Time 6-23
Host interface 2-21
Host Services A-3

hostname 2-2, 6-2
how rising and falling thresholds work 3-6
hysteresis 3-6

I

IETF MIBs, supported by EMM-E6 A-1
IF Number 3-4
IF Type 3-4
IfIndex 6-12
ifInErrors 3-4
ifInOctets 3-4
In Octets Kb 3-3
Info button
    bridge 6-5
In—Out—In box 6-33
Interface display mode 2-6
Interface Number 2-17
invalid entry status 6-15
IP address 2-3, 6-4
IP Services A-2

J

Jabbers 2-19

L

Learned Entry Discards 6-15
learned entry status 6-15
LEM Count 4-6, 4-12
LEM Rate 4-8
LEM Reject Count 4-6
LEM Reject Rate 4-8
LER Alarm 4-9, 4-11
LER Cutoff 4-9, 4-12
LER Estimate 2-9, 4-7, 4-9, 4-11
Link Status 2-16
Load
    Ethernet (RMON) 2-19
    MIB II 2-17
Log 3-4
log files
    saving 6-35
logDescription 3-11
logEventIndex 3-10
logIndex 3-10
logTime 3-11

M

MAC Address 4-25, 6-5
management entry status 6-15
manipulating the Hub View display 2-2
Max Age 6-22
Max Connections 2-24
maximum log entries 6-34
maximum transfer unit 6-13
Media Type 4-4
Menus
    always available 2-6
    Bridge mode 2-6
    Interface mode 2-6
    Switch mode 2-6
Meters tool
    accessing 6-27
MIB component A-1
    descriptions A-4
MIB I, II 1-4, 2-3, 2-26
MIB II variables 3-4
MIB Navigator A-3
MIBTree 1-4
Module Index 2-5
Module menu 2-7
Module Type 2-5
MSB (Ethernet) address mode 4-25
MtuExceedDiscard 6-13

N

Node Class 4-26
notification conditions 6-31
notification options 6-31
Nucast (non-unicast) 2-18
Num Connections 2-24
Number of Topology Changes 6-22

O

Once only 6-33
open the Filtering Database window 6-14
Oper State
    Interface 2-16
    Switch 2-11
other entry status 6-15

P

Packets/second 2-19
Path 1-4
Path Cost 6-25

Path Tool 2-26
Percentage button 6-7, 6-8
permanent entry status 6-16, 6-19
Permanent Virtual Circuits (PVCs) 5-1
Pie Chart tool
    accessing 6-27
Polling Intervals 2-4, 2-28, 3-5
    editing 6-36
Port
    Changing Path Cost 6-27
    Changing Priority 6-27
    Designated 6-27
    Designated Cost 6-26
    Path Cost 6-25
Port Configuration (FDDI) 2-27
Port Display Form 2-5
Port Index 2-5, 4-3, 4-11
Port Number 3-4
Port State 4-4
Port Status 2-5
Port Type
    FDDI 2-9
    Interface 2-17
    Switch 2-12
PortCircuit 6-12
Priority 6-23
Priority (Port) 6-25

Q

Quit button
    bridge 6-5

R

Receive Port 6-15
Remain—In box 6-33
rising action 3-5, 3-8
rising alarm threshold 3-1
rising threshold 3-5, 3-7, 3-8
RMON Default A-3
RMON MIB component 3-2
Root
    Cost 6-23
    Forward Delay 6-24
    Hello Time 6-24
    Max Age 6-24
    Port 6-23
Root Bridge 6-20
    selection process 6-20

S

SecureFast switching 1-2, 2-10, 2-26
self entry status 6-15
Send Mail 6-32
set bridge port thresholds 6-31
Sfs Admin Status 2-23
Sfs Operating Status 2-24
SMT Connection Policy 2-28
SMT Index 2-10, 4-3, 4-10
SMT/MAC Configuration 2-28
Software Version 2-21
Source Address 6-15
Source Routing button 6-8
Spanning Tree Algorithm (STA) 6-2, 6-20
    version 6-21
Spanning Tree Port Table 6-26
    accessing 6-25
Spanning Tree Protocol window 6-21
    accessing 6-21
Speed 2-17
SPMA Tool applications 2-25
spmarun 2-1, 3-2, 4-2, 4-9, 4-13, 4-21, 4-24, 5-1, 6-2
Sr Frames Forwarded 2-14
static entry 6-13
Station List 2-28
Statistics
    Ethernet (RMON) 2-18
    MIB II 2-17
Status (alarm) 3-4
Switch display mode 2-6
SWITCH Services A-3
Switched Virtual Circuits (SVCs) 5-1
sysUpTime 3-11

T

Technical Support 1-8
Telnet 1-4, 2-26
TFTP Download 1-4, 2-26
threshold pairs 3-6
Top Level Serial Number 2-21
Topology 4-26
Topology Change flag 6-22
Total Errors 3-3
Tp Frames forwarded and filterd 2-14
traditional bridging 2-13, 2-26, 2-28, 2-38
traditional switching (or bridging) 1-2
Transparent Bridge A-2
Transparent button 6-8

Trap 3-5
Trap Table 1-4, 2-26

U

unique community names A-3
unused resources 3-9
UPS 1-4
    configuration tool 2-27
Uptime 6-4

V

VC MUX 802.3 Bridging 5-4
viewing an alarm log 3-1, 3-5, 3-10
Virtual Channel Identifier (VCI) 5-3
Virtual Path Identifier (VPI) 5-3

W

Web site 1-8